

BOLETÍN

Ciberseguridad en un PAC

Tendencias y retos
cibernéticos para los PACs

Riesgos por ataques cibernéticos
más frecuentes

Principales amenazas de seguridad
cibernética 2024-2025

Índice

Edición Enero-Febrero

P. 4

Importancia de
ciberseguridad en un PAC

P. 6

Tendencias y retos cibernéticos
para los PACs

P. 8

Riesgos por ataques
cibernéticos más frecuentes

P. 12

Principales amenazas de
seguridad cibernética 2024-
2025

P. 16

Ciberseguridad en PACs

P. 20

Riesgos cibernéticos incluyendo
PACs

P. 24

Noticias Amexipac

P. 28

Plan Maestro del SAT

P. 30

Hecho en México: El sello
que impulsa la identidad y
competitividad de los productos
mexicanos

P. 32

¿Cuál será el futuro de la Inteligencia
Artificial en las Administraciones
Tributarias?



P. 38

Detección del lavado de dinero con ayuda de la IA

P. 44

Ya no basta solo el CFDI

P. 40

Beneficios y desafíos de los impuestos ecológicos en economías emergentes

P. 46

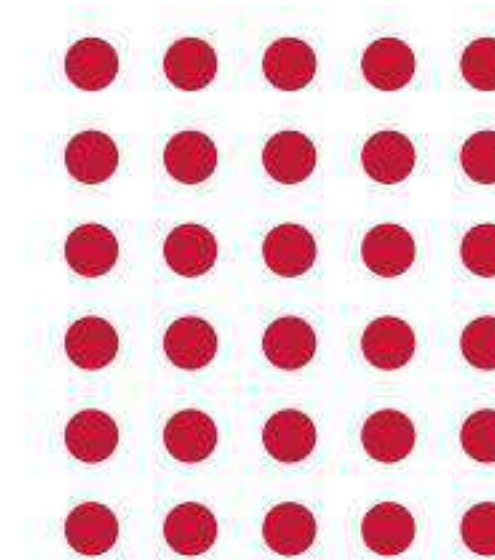
¿Qué es el Sistema de Información de Subcontratación (SISUB)?

Editorial

Dirección editorial:
Amexipac, A. C.

Arte y diseño:
TresDigital Reputation Care
S.A de C.V.

Amexipac, A.C. © todos los derechos reservados 2023. Ni la totalidad ni parte de esta publicación puede ser reproducida o almacenada en un sistema de recuperación o ser transmitido en cualquier forma ya sea electrónica, óptica, mecánica fotocopia, magnética, grabación o cualquier otro medio sin previa autorización por escrito de Amexipac, A.C. Para cualquier aclaración por favor contáctenos en el correo electrónico info@amexipac.org.mx. El contenido e información aquí provista es integrada o desarrollada con fines informativos exclusivamente y no constituye una opinión profesional, fiscal o legal por lo que Amexipac, a.c. no asume ninguna responsabilidad sobre su uso.



Importancia de ciberseguridad en un PAC

Ana Navarro



La ciberseguridad es un tema fundamental en todo el mundo y México no es la excepción. A medida que la tecnología avanza más personas, empresas y gobiernos dependen de sistemas digitales, convirtiendo la ciberseguridad en un pilar esencial ya que protege los sistemas, redes y datos frente a amenazas cibernéticas. No solo es una cuestión técnica, sino una estrategia integral que debe abarcar tecnología, procesos y concienciación.

Los Proveedores Autorizados de Certificación (PACs) ejercen una función fundamental en la gestión de los documentos fiscales en México. Estos servicios no solo garantizan la emisión adecuada de los Comprobantes Fiscales Digitales por Internet, sino que también manejan una gran cantidad de información sensible y confidencial. La protección de los datos se convierte en una prioridad para evitar ataques que podrían comprometer la **integridad, confidencialidad y disponibilidad de la información**.

El manejo adecuado de la ciberseguridad en los PACs es crucial principalmente por las siguientes razones:

1. Protección de datos sensibles:

Los PAC almacenan y procesan información altamente sensible, como datos personales de contribuyentes y empresas, registros financieros, etc. La protección de esta información es esencial para evitar el robo de identidad, fraude fiscal y la manipulación de datos.

2. Integridad de la información:

La integridad de la información en un PAC es la capacidad de garantizar que los datos transmitidos y almacenados, relacionados con los comprobantes fiscales digitales, no hayan sido alterados, manipulados o dañados de forma no autorizada.

El cifrado de datos y las autenticaciones robustas ayudan a prevenir la alteración o manipulación de la información.

3. Disponibilidad de los servicios:

La disponibilidad de los servicios de los PACs es fundamental para la eficiencia, seguridad y legalidad de las operaciones fiscales en el contexto de la facturación electrónica. Los contribuyentes y empresas dependen de la fiabilidad de estos proveedores para cumplir con obligaciones fiscales y mantener sus actividades comerciales sin interrupciones.

Para evitar interrupciones, es necesario implementar medidas de protección robustas que garanticen la continuidad de los servicios.

4. Cumplimiento normativo:

Los sistemas fiscales y de control de datos, como los PAC, deben cumplir con diversas regulaciones de seguridad informática y protección de datos personales. Esto incluye normativas locales e internacionales. La ciberseguridad es clave para asegurar que las instituciones cumplan con normativas y evitar sanciones.

5. Confianza del usuario:

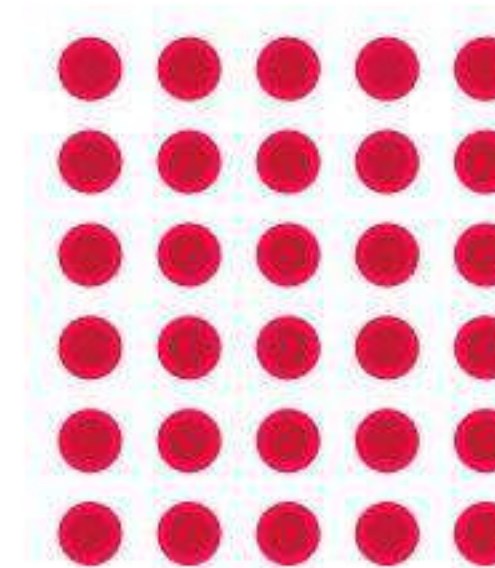
La implementación de fuertes protocolos de seguridad cibernética aumenta la confianza de los usuarios en los sistemas, incentivando el cumplimiento voluntario de las obligaciones fiscales.



En resumen, la ciberseguridad es una necesidad tecnológica y estratégica para proteger la información, asegurar la operatividad de los sistemas y mantener la confianza en las plataformas digitales.

El boletín explora la importancia de la ciberseguridad en los PAC y las amenazas a las que se enfrentan, además de las herramientas necesarias para su protección y el impacto que podría tener un incidente de seguridad en sus operaciones.





Tendencias y retos cibernéticos para los PACs

Ana Navarro



Los Proveedores Autorizados de Certificación (PACs), han continuado adaptándose a los desafíos en términos de ciberseguridad, dada la creciente amenaza de ciberataques que afectan no solo a las empresas, sino también a las instituciones que gestionan la validación y emisión de documentos fiscales.

Tendencias relevantes de PAC EN 2024:

Los Proveedores de Certificación de Comprobantes Fiscales Digitales por Internet, conocidos como PACs, han continuado adaptándose a los desafíos en términos de ciberseguridad, dada la creciente amenaza de ciberataques que afectan no solo a las empresas, sino también a las instituciones que gestionan la validación y emisión de documentos fiscales.

1. Fortalecimiento de protocolos de seguridad:

El Servicio de Administración Tributaria (SAT) en México y los PAC implementan protocolos de seguridad para proteger la integridad de los datos de las transacciones electrónicas y la emisión de CFDIs. Estos protocolos incluyen encriptación avanzada, autenticación de dos factores y otros métodos de protección para asegurar que los datos fiscales no sean vulnerados por ataques cibernéticos.



2. Regulaciones más estrictas:

Las normativas internacionales como ISO 27001, NIST, así como los estándares nacionales de protección de datos, han ganado relevancia. Los Proveedores de Certificación de Comprobantes Fiscales están adoptando estas regulaciones con mayor rigor, con el objetivo de blindar sus operaciones frente a un panorama de amenazas cada vez más complejo.

3. Innovación en soluciones de seguridad:

Las herramientas basadas en inteligencia artificial y machine learning están expandiéndose y tomando fuerza. Estas tecnologías permiten a los Proveedores de Certificación de Comprobantes Fiscales detectar patrones sospechosos y prevenir ataques antes de que ocurran, optimizando la protección de datos.

Retos para los PAC en 2025:

1. Resiliencia ante ciberataques:

Ciber resiliencia: Desarrollar capacidades para prevenir, detectar y responder a ciberataques rápidamente será fundamental. Las plataformas deben integrar procesos de recuperación ante desastres y de continuidad del negocio (BCP/DRP) que minimicen los efectos de un ataque a gran escala.

Ciberseguridad en la cadena de suministro: Con el aumento de ataques a través de proveedores, las plataformas deben ser capaces de detectar y prevenir riesgos en la cadena de suministro de TI, protegiendo sus sistemas.

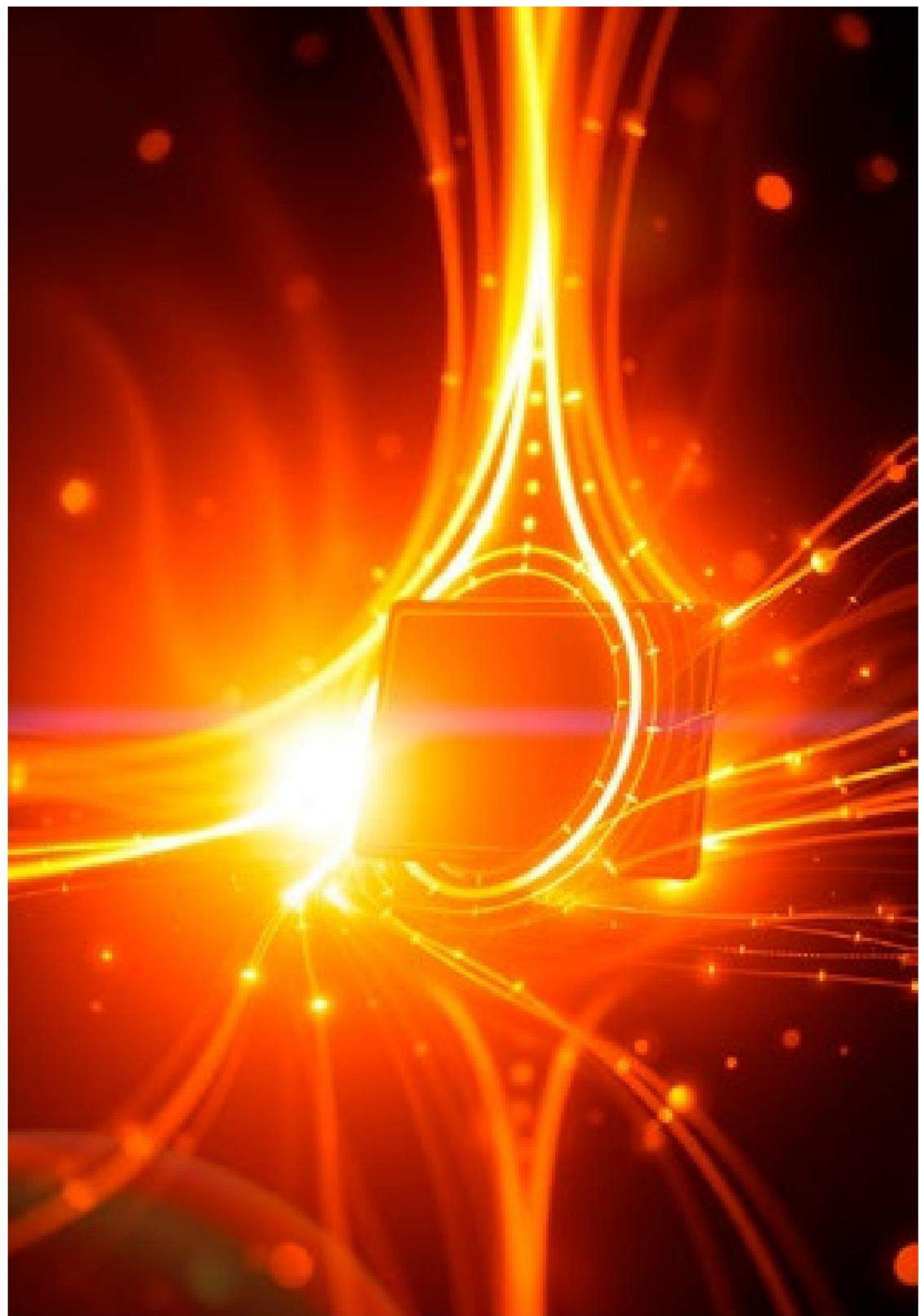
2. Ciberataques más avanzados:

Los ataques cibernéticos seguirán evolucionando, con métodos más complejos, como el uso de inteligencia artificial (IA) y aprendizaje automático para automatizar y mejorar la precisión de los ataques.

El “phishing” y el “ransomware” seguirán siendo amenazas significativas, con variantes cada vez más difíciles de detectar.

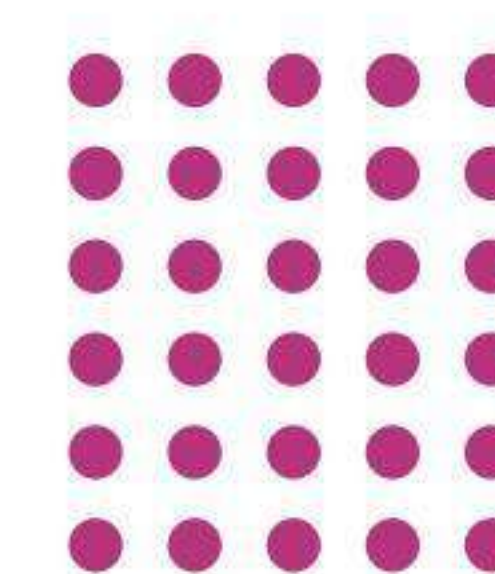
3. Automatización y respuesta ante incidentes:

Las organizaciones tendrán que adoptar tecnologías que les permitan responder más rápidamente y de manera más eficaz a los incidentes de seguridad. Las soluciones automatizadas de respuesta ante incidentes (con IA y análisis predictivo) jugarán un papel clave en la detección temprana y la mitigación de ataques.



La ciberseguridad en 2025 exigirá un enfoque proactivo, una mayor colaboración entre gobiernos, empresas y ciudadanos, y una constante adaptación a nuevas amenazas.





Riesgos por ataques cibernéticos más frecuentes

Ricardo Hernández



En el mundo hiperconectado en el que vivimos y con los crecientes usos de tecnología para resguardo de datos confidenciales o sensibles, los ciberataques se han convertido en una de las principales amenazas para las organizaciones y las personas. A continuación, se describen los riesgos más frecuentes derivados de estos ataques, así como sus posibles consecuencias y mitigaciones.



1. Phishing

El phishing implica engañar a las víctimas para que proporcionen información confidencial, como datos personales o bancarios, a través de mensajes fraudulentos que aparentan ser de fuentes confiables. Este tipo de ataque es común y ha mostrado un incremento significativo en los últimos años.

Riesgos:

- Robo de identidad.
- Acceso no autorizado a cuentas bancarias.
- Pérdida de datos sensibles.

Medidas de mitigación:

- Educar a los usuarios sobre la identificación de correos y mensajes sospechosos.
- Implementar filtros de correo electrónico avanzados.
- Utilizar autenticación multifactor en cuentas sensibles.

2. Ransomware

El ransomware es un software malicioso que cifra los datos de la víctima y exige un pago para restaurar el acceso. Se ha observado un aumento en este tipo de ataques, afectando tanto a empresas como a instituciones gubernamentales.

Riesgos:

- Interrupción de operaciones críticas.
- Pérdidas financieras significativas.
- Daño a la reputación de la organización.

Medidas de mitigación:

- Realizar copias de seguridad periódicas y almacenarlas de forma segura.
- Mantener el software y los sistemas operativos actualizados.
- Implementar soluciones de seguridad que detecten y bloqueen malware.

3. Ataques DDoS (Denegación de Servicio Distribuida)

Los ataques DDoS buscan saturar los recursos de una red o servicio, haciéndolos inaccesibles para los usuarios legítimos. Estos ataques han aumentado, afectando la disponibilidad de servicios en línea.

Riesgos:

- Caída de sitios web o aplicaciones.
- Pérdida de ingresos por interrupción del servicio.
- Costos elevados en mitigación y recuperación.

Medidas de mitigación:

- Implementar soluciones de balanceo de carga.
- Utilizar servicios de mitigación de DDoS proporcionados por proveedores especializados.
- Monitorear el tráfico de red para detectar anomalías.

4. Inyección de código (SQL Injection)

Este ataque explota vulnerabilidades en aplicaciones web para insertar código malicioso en consultas SQL, permitiendo el acceso no autorizado a bases de datos. Las empresas mexicanas no están exentas de este riesgo, especialmente aquellas con sistemas web desactualizados.

Riesgos:

- Robo de información confidencial.
- Alteración o eliminación de datos.
- Exposición de información personal de clientes.

Medidas de mitigación:

- Validar y sanitizar todas las entradas de usuario en las aplicaciones web.
- Utilizar consultas parametrizadas y procedimientos almacenados.
- Realizar pruebas de penetración periódicas para identificar vulnerabilidades.

5. Malware

El malware incluye diversos tipos de software malicioso, como virus, gusanos y troyanos, diseñados para dañar o infiltrarse en sistemas informáticos. En México, la proliferación de malware ha sido notable, afectando tanto a usuarios individuales como a organizaciones.

Riesgos:

- Daño o destrucción de archivos.
- Pérdida de datos importantes.
- Monitoreo no autorizado de la actividad del usuario.

Medidas de mitigación:

- Instalar y mantener actualizado un software antivirus confiable.
- Evitar descargar software de fuentes no confiables.
- Actualizar regularmente todos los programas y sistemas operativos.

6. Ataques de fuerza bruta:

En estos ataques, los ciberdelincuentes intentan acceder a cuentas probando múltiples combinaciones de contraseñas hasta encontrar la correcta. Este método sigue siendo utilizado en México para comprometer cuentas personales y corporativas.



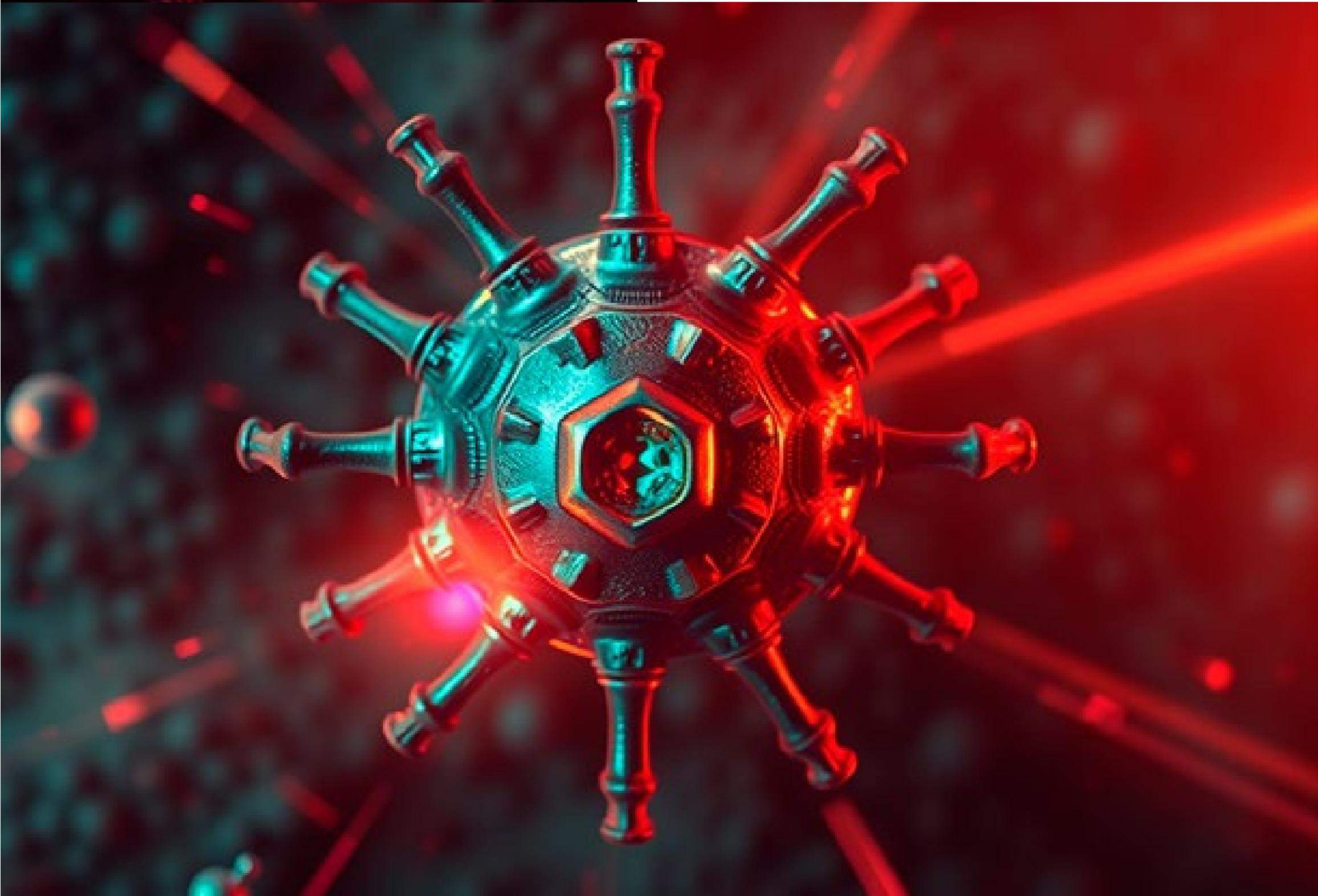


Riesgos:

- Acceso no autorizado a sistemas o cuentas.
- Robo de información confidencial.
- Compromiso de recursos internos.

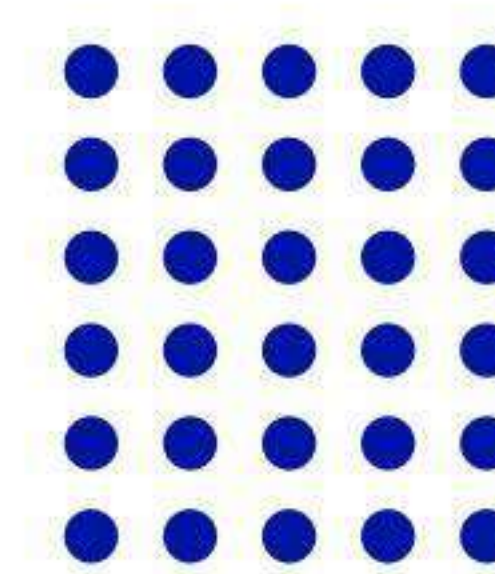
Medidas de mitigación:

- Utilizar contraseñas robustas y únicas para cada cuenta.
- Implementar autenticación multifactor.
- Limitar el número de intentos de inicio de sesión fallidos.



Se recomienda todas las organizaciones incluyendo a los PACs, tengan protocolos, herramientas y controles de ciberseguridad para evitar o minimizar riesgos de alto impacto.





Principales amenazas de seguridad cibernética 2024-2025

Erick Romero



En un mundo donde la digitalización se ha convertido en una parte fundamental de nuestras vidas y operaciones, las amenazas a la ciberseguridad han evolucionado a un ritmo alarmante, presentando riesgos significativos para individuos, organizaciones e infraestructuras críticas. A continuación, se presentan las 10 principales amenazas de seguridad cibernética incluyendo las previstas para 2025:

1. Ataques de ingeniería social:

La ingeniería social es una táctica utilizada por los cibercriminales para manipular psicológicamente a las personas y que compartan su información privada. Se hacen pasar por alguien conocido o de confianza para que revelen información confidencial y así acceder a sus cuentas personales, financieras o laborales. Existen varios tipos de ataques de ingeniería social, como el phishing, el vishing, el smishing y el pretexting.

El phishing suele producirse por correo electrónico. Los cibercriminales enviarán un correo electrónico de phishing con un enlace o archivo adjunto cuyo objetivo es que la víctima haga clic en él o lo descargue. Sin embargo, si la víctima llega a hacer clic en el enlace o descarga

el archivo adjunto no solicitado, podría estar descargando malware en su dispositivo y provocar así el robo de su información privada por parte de un cibercriminal.

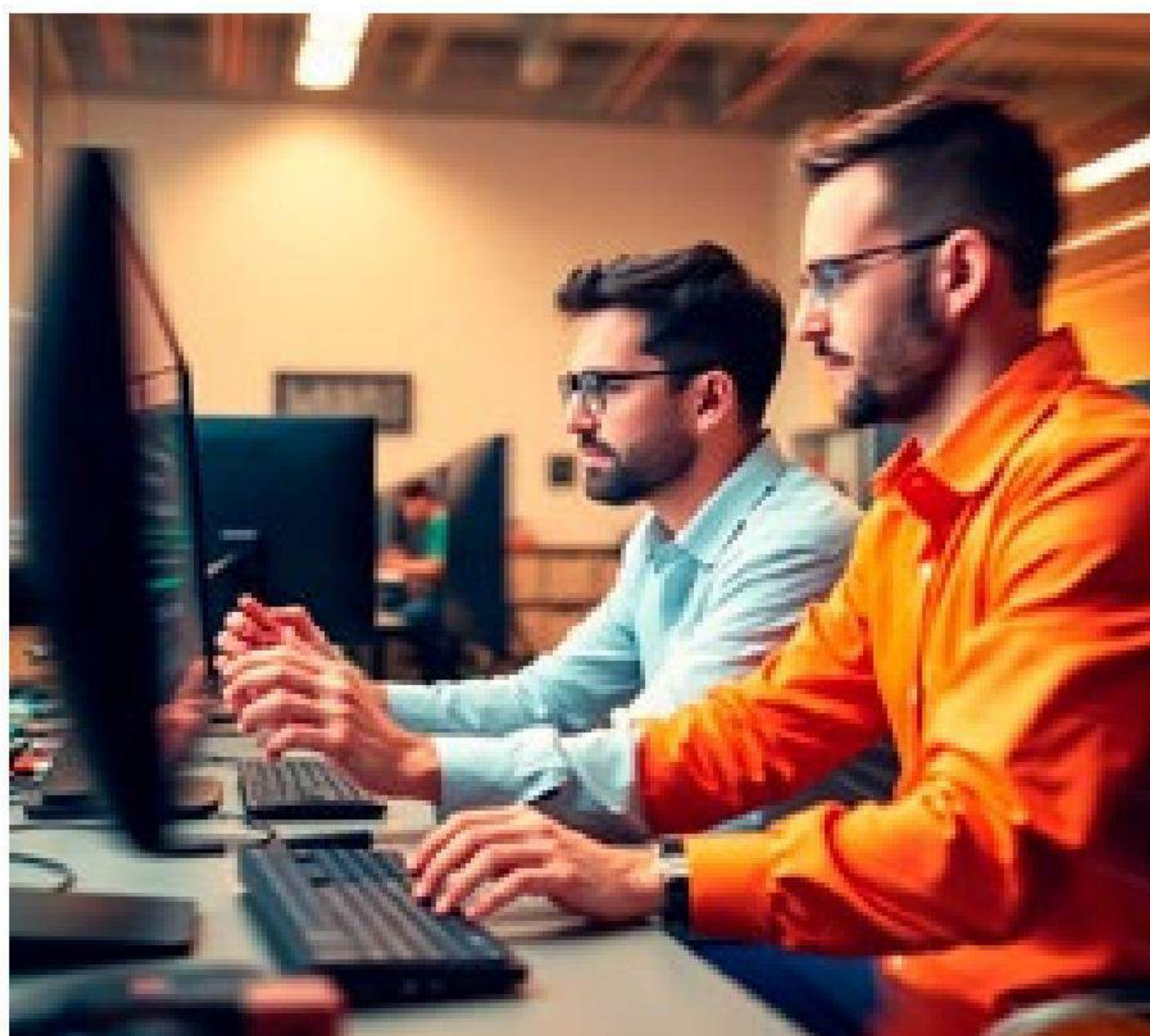
El vishing y el smishing son similares al phishing, pero el vishing se hace por teléfono y el smishing se hace por medio de mensajes de texto.

El pretexting consiste en que el cibercriminal genere una historia u ofrezca un pretexto que haga que la víctima sienta lástima o miedo, y esto haga que comparta información personal.

La solución consiste en proporcionar formación y capacitación continua a los usuarios y en establecer filtros más especializados.

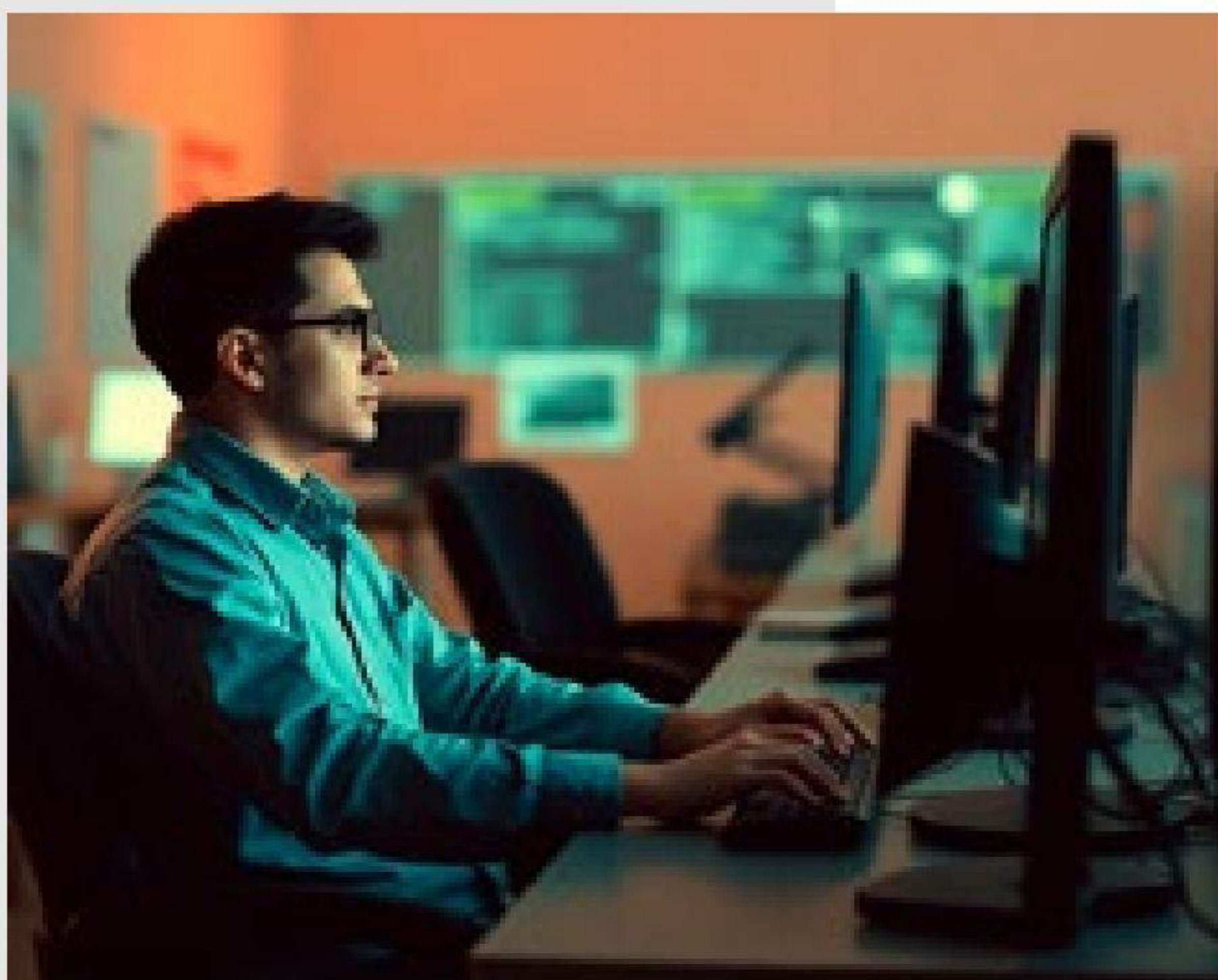
2. Ransomware avanzado y extorsión:

Los ataques de ransomware han incrementado su sofisticación, dirigiéndose especialmente hacia infraestructuras críticas, como hospitales, redes eléctricas y entidades gubernamentales. Además del cifrado de datos, los ciberdelincuentes han adoptado la estrategia de doble extorsión, amenazando con publicar los datos si no se paga el rescate. La solución radica en implementar medidas de ciberseguridad efectivas que permitan detectar y mitigar estos ataques antes de que ocurran.



3. Ataques a la cadena de suministro:

En lugar de centrarse en empresas específicas, los cibercriminales tienden a atacar a **proveedores y/o distribuidores** a través de ataques a la cadena de suministro. Uno de los ataques más conocidos a la cadena de suministro se produjo en 2019 e involucró a Orion, el software de SolarWinds. Los cibercriminales insertaron su malware mediante código en las actualizaciones del software y, cuando las organizaciones se descargaron la nueva actualización los cibercriminales consiguieron acceder a miles de sistemas, lo que les permitió espiar a otras organizaciones. Dado que la mayoría de las cadenas de suministro son extensas y multicapa, es difícil descubrir dónde se encuentran las debilidades de seguridad tras un ataque cibernético de este tipo.



4. Malware sofisticado:

Herramientas maliciosas como XWorm y AsyncRAT están diseñadas para explotar vulnerabilidades y permitir a los criminales acceder de manera remota a sistemas comprometidos. Este tipo de malware puede desactivar programas de seguridad, registrar pulsaciones de teclas y robar información sensible. Las organizaciones deben actualizar sus programas y utilizar herramientas de detección de amenazas.

5. Amenazas a dispositivos IoT:

A medida que los dispositivos inteligentes van ganando popularidad, los cibercriminales encuentran maneras de atacar a toda una variedad de objetos físicos con conexión a Internet. En lo que suele conocerse como un ataque al Internet de las cosas (IoT), los cibercriminales que consigan acceder a su red Wi-Fi también podrían conectarse a sus dispositivos inteligentes y robar allí sus datos privados. Además de las computadoras, celulares y tabletas tradicionales, pueden ser los dispositivos inteligentes que hay en casa, como el Amazon Echo, el Ring Timbre, el termostato Nest o el monitor para bebés Nanit. Estos dispositivos inteligentes, y muchos otros, podrían ser infectados con malware si un cibercriminal logra conectarse a ellos, lo que les permitiría robar su información personal o incluso espiarle a través de la cámara o el micrófono del dispositivo.

Los ataques de IoT pueden ser increíblemente invasivos y traumáticos para cualquiera cuando se dan cuenta de que los cibercriminales pueden ver y escuchar todo lo que hacen. Es crucial proteger estos dispositivos mediante redes con contraseñas seguras, actualizaciones de software regulares y segmentación de redes.

6. Ataques impulsados por la IA:

La inteligencia artificial se ha utilizado no solo para la defensa, sino también con fines maliciosos. Los cibercriminales emplean IA para automatizar ataques, realizar distorsiones profundas y detectar vulnerabilidades. Invertir en sistemas de IA que ayuden a predecir y prevenir estos ataques es esencial.

Según un informe de Deep Instinct, el 85 % de los ataques cibernéticos en 2024 han utilizado la IA. Los cibercriminales están evolucionando en sus técnicas para utilizar la IA como herramienta para ataques cibernéticos como el vishing. Hay otras formas en que los cibercriminales cometen ataques con IA, por ejemplo, para descifrar contraseñas.

7. Desinformación y robo de identidad digital:

Los servicios de desinformación han aumentado notablemente. Los delincuentes utilizan IA para crear perfiles falsos y suplantar identidades, lo que les permite realizar compras y transacciones en línea. Proteger la identidad digital requiere autenticación multifactor y un control de acceso riguroso.

8. Vulnerabilidades en la Nube:

Dado que cada vez son más las organizaciones y los usuarios que confían en sistemas o dispositivos basados en la nube, existen muchas vulnerabilidades o debilidades dentro de estos sistemas que pueden ser aprovechadas por los cibercriminales. Según un informe de IBM de 2024, más del 40 % de las violaciones de datos se producen en la nube y la recuperación de las empresas puede costar millones de dólares. Las vulnerabilidades en la nube pueden tener

consecuencias que van más allá de las pérdidas financieras, puesto que la vulneración de los datos de los clientes puede provocar la desconfianza de los mismos y daños en la reputación frente a los potenciales clientes futuros.

Uno de los mayores tipos de vulnerabilidades en la nube que puede sufrir una organización es la configuración errónea de esa misma nube; que los recursos en la nube no estén configurados o siendo gestionados correctamente, lo que provoca fallos de seguridad y abre la puerta a la posibilidad de que se produzcan violaciones de datos. Por lo general, si los empleados solo disfrutan de un acceso con privilegios mínimos, los cibercriminales no podrán atacar a la empresa a gran escala en el caso de que se produzca una violación de seguridad, puesto que los empleados solo tendrán acceso a lo estrictamente necesario para hacer su trabajo.

9. Ataques por vulneración en correos electrónicos empresariales (BEC):

Los empleados podrían ser objeto de un ataque en el que un cibercriminal se haría pasar por una figura autorizada dentro de la empresa, como el director general, para engañar a sus empleados y que les envíen dinero o información privada. Dado que los cibercriminales necesitan saber a quién atacar y la identidad de quién deben suplantar, este tipo de ataque cibernético requiere una gran labor de investigación para conseguir generar la suficiente confianza y pasar desapercibidos.

10. Ataques de denegación de servicio distribuido (DDoS):

Estos tienen por objetivo perturbar el tráfico normal de un servidor, provocando tal sobrecarga que éste termine por bloquearse. Los cibercriminales harán esto con el fin de dañar la reputación de una organización, pedir un rescate para dejar de saturar el tráfico o detener por completo el normal funcionamiento de un sitio web para provocar el caos. Dado que

las redes tienen un límite de solicitudes que pueden ser gestionadas de forma simultánea, los ataques DDoS dependen de bots para llevar a cabo sus ataques masivos, que saturan la red con solicitudes y, a la larga, detienen el tráfico por completo. Si bien esta no es una de las amenazas cibernéticas más conocidas, los ataques DDoS han ido en aumento y pueden causar la ruina financiera de una organización.

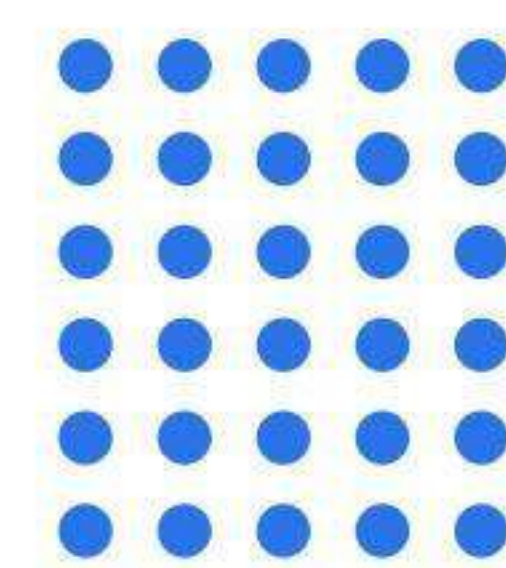
En conclusión:

Para enfrentar estas amenazas, las organizaciones deben adoptar un enfoque proactivo. Esto implica implementar sistemas de protección avanzados, organizar sesiones de actualización para los empleados y mantener una colaboración continua con organismos de ciberseguridad. De esta manera, se podrán seguir utilizando datos y operando de forma segura frente a futuros delitos digitales.





Ciberseguridad en PACs



Beatriz Muñoz



Como sabemos, la **ciberseguridad** cada vez ha tomado más importancia e impacto en las organizaciones. Más allá de lo que solicita y audita la autoridad a los PACs (Proveedores Autorizados de Certificación) por medio de sus matrices de control, diversos marcos de referencia de calidad, ciberseguridad y seguridad de la información como ISO 27001, NIST, COBIT, hacen hincapié y cuestionan en cómo se protegen los datos de los contribuyentes (clientes), cómo evitar la manipulación o robo de éstos, además de auditar qué protocolos de protección tecnológica tiene el PAC para evitar ataques cibernéticos que pueden terminar en una fatalidad por medio de *phishing*, *el vishing*, *el smishing* y *el pretexting*, *Cross Site Scripting*, *Inyección SQL*, *Ransomware*, *Drive-by*, *Suplantación de identidad*, *Malware*, entre otros.

La ciberseguridad es esencial para los **PACS**, por lo cual se recomienda de forma general, tener implementados los siguientes protocolos de seguridad, algunos de ellos incluidos en la *Matriz de 86 Controles para la Revisión de Seguridad del SAT*.

1. Protección de la información sensible:

- **Encriptación de datos:** Asegurarse de que toda la información sensible esté encriptada tanto en tránsito como en reposo (Control 85).
- **Control de acceso:** Implementar políticas estrictas de control de acceso a los sistemas que contienen datos confidenciales. Utilizar autenticación multifactor (MFA) para acceder a plataformas sensibles (Control 44 y 78).
- **Clasificación de la información:** Definir claramente qué información es sensible y cuál puede ser de acceso público, asegurando que los datos no se filtren accidentalmente (Control 8).
- **Uso de contraseñas:** La empresa debe contar con una política de uso de contraseñas, donde se especifique la responsabilidad de los usuarios en el uso de estas, vigencia, protección de ellas, etc. (Control 15). En el caso del aplicativo de facturación electrónica, se recomienda se exija el cambio frecuente de contraseñas al usuario (contribuyente).

2. Seguridad en la red

- **Firewalls y sistemas de detección de intrusos (IDS/IPS):** Implementar firewalls robustos y sistemas de detección para identificar actividades sospechosas y prevenir intrusiones (Controles 58 y 74).
- **Redes privadas virtuales (VPN):** Garantizar que las conexiones remotas, especialmente las de empleados o auditores externos, utilicen VPNs seguras para prevenir interceptaciones (Controles 44 y 45).
- **Segmentación de redes:** Asegurarse de que las diferentes redes que maneja el PAC estén segregadas para limitar el impacto en caso de un ataque (Control 60).



3. Resiliencia y planificación ante incidentes

- **Planes de respuesta a incidentes:** Establecer protocolos claros para actuar ante ciberataques o violaciones de datos. Esto incluye identificar, contener, mitigar y recuperar de posibles ataques (Controles 28 y 29).
- **Copias de seguridad (backups):** Realizar copias de seguridad periódicas y almacenarlas en entornos seguros para evitar la pérdida de datos críticos durante un ataque, como un ransomware (Controles 63 y 64).
- **Pruebas de resiliencia:** Realizar simulacros periódicos de ciberseguridad para comprobar que los sistemas pueden resistir ataques y que los equipos saben cómo responder.

4. Gestión de vulnerabilidades

- **Actualizaciones y parches:** Mantener todos los sistemas y software actualizados para protegerse contra vulnerabilidades conocidas. Los parches deben aplicarse de manera inmediata (Control 62).
- **Auditorías de seguridad regulares:** Realizar auditorías internas y externas periódicas para identificar brechas de seguridad y debilidades en la infraestructura (Controles 71 y 72).

5. Seguridad en el desarrollo de Software

- **Desarrollo seguro (DevSecOps):** Incorporar la seguridad desde las fases iniciales del desarrollo de software, asegurándose de que no se introduzcan vulnerabilidades en el código (Control 61).
- **Revisión de código y pruebas de penetración:** Realizar revisiones de seguridad regulares y pruebas de penetración para detectar posibles fallos (Controles 71).



6. Educación y concientización:

- **Entrenamiento continuo:** Formar a los empleados del PAC en mejores prácticas de seguridad cibernética, como evitar el phishing, crear contraseñas seguras y reconocer amenazas cibernéticas. (Controles 12).
- **Simulacros de phishing:** Realizar campañas de simulacro de phishing para enseñar a los empleados a reconocer correos electrónicos maliciosos o enlaces comprometidos (Controles 12).

7. Cumplimiento normativo

- **Cumplimiento con regulaciones de protección de datos:** Asegurarse de que el PAC cumpla con normativas de privacidad y protección de datos acorde a lo estipulado en la Ley Federal De Protección de Datos Personales en Posesión de los Particulares, o regulaciones locales aplicables ejemplo con INAI (Controles 4).
- **Monitoreo de actividades de cumplimiento:** Implementar sistemas que ayuden a monitorear y garantizar que las prácticas del PAC cumplan con todas las normativas de seguridad relevantes.

8. Protección ante amenazas avanzadas

- **Inteligencia de amenazas:** Utilizar herramientas de inteligencia de amenazas para identificar y mitigar ataques avanzados, como los dirigidos (APT), que pueden estar enfocados en infiltrarse en las redes del PAC.
- **Análisis de comportamiento:** Implementar herramientas de análisis de comportamiento para identificar anomalías que puedan indicar una amenaza interna o un compromiso de la seguridad.

9. Colaboración con otros organismos

- **Compartir información sobre amenazas:** Colaborar y participar con otras instituciones gubernamentales y organizaciones del sector privado para compartir información sobre amenazas y mejores prácticas en ciberseguridad. (Controles 6).

10. Monitoreo continuo

- **Supervisión de redes 24/7:** Implementar sistemas de monitoreo continuo para detectar actividad inusual o potencialmente peligrosa en la infraestructura tecnológica del PAC. (Controles 31 y 32).
- **Análisis forense:** Establecer capacidades para realizar análisis forenses en caso de incidentes, para entender cómo se produjo un ataque y evitar su recurrencia (Controles 28).

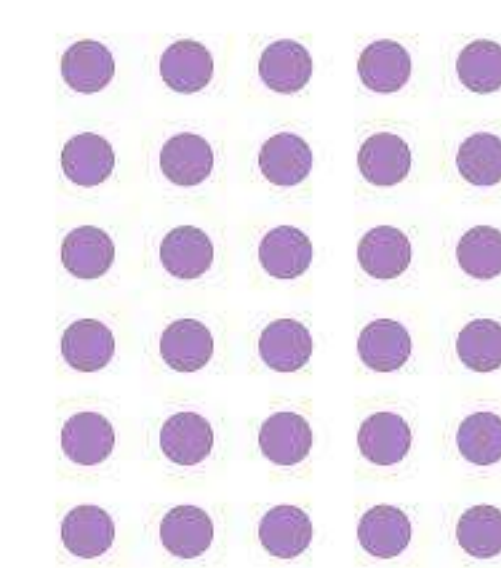
En conclusión:

Los PAC deben tener una estrategia integral de ciberseguridad actualizada que abarque la protección de la información, la resiliencia ante ataques, la gestión de vulnerabilidades, la educación constante del personal, el cumplimiento de normas y la colaboración interinstitucional para enfrentar las amenazas cibernéticas de forma efectiva, asegurando así su integridad y la información de terceros.

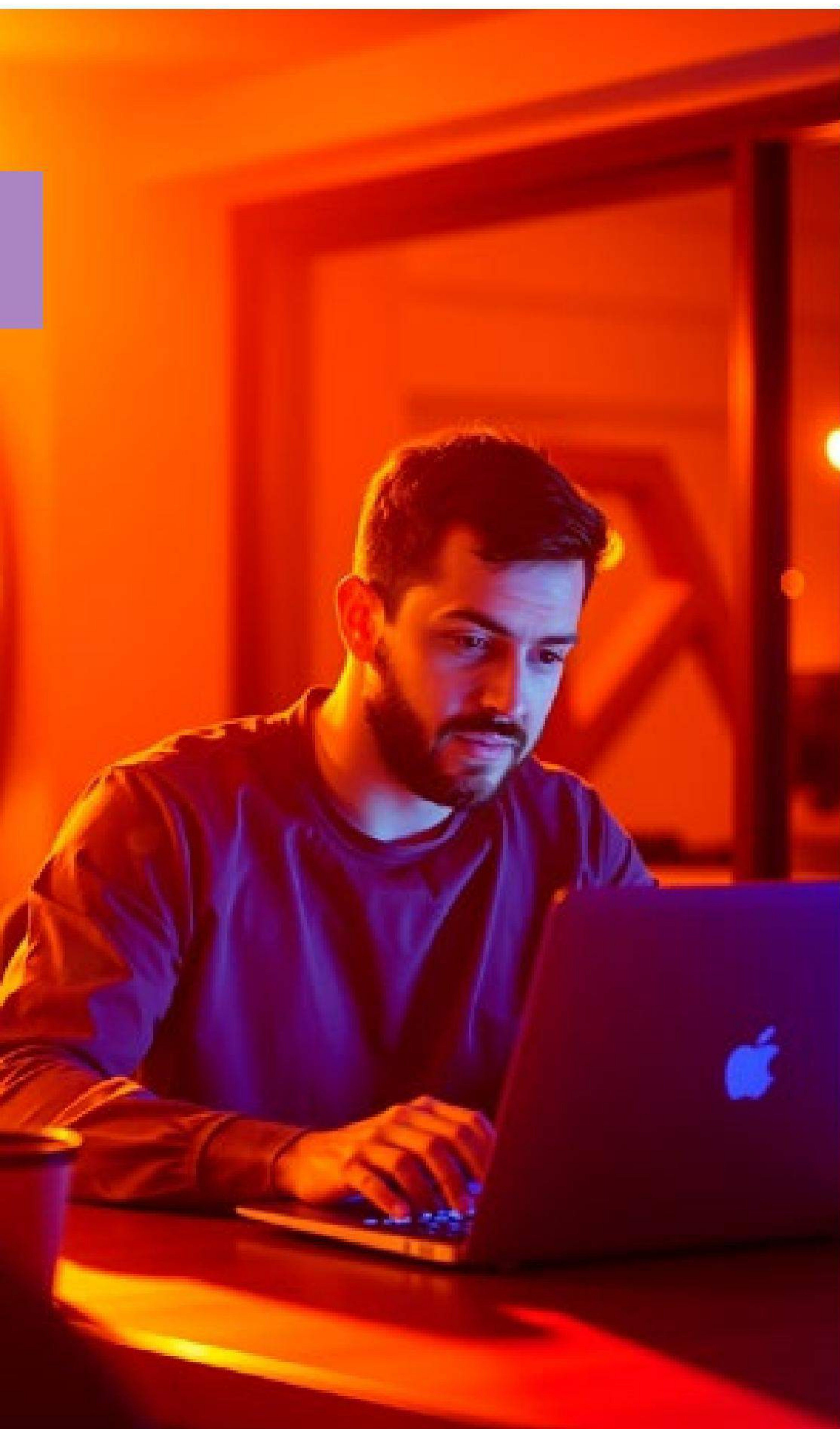
Se exhorta a mantenerse informados y capacitados en tendencias, noticias y riesgos de México y el mundo.



Riesgos cibernéticos incluyendo PACs



Beatriz Muñoz



De acuerdo con El Economista, **México se enfrenta a un incremento notable en los ataques cibernéticos**. Durante el tercer trimestre de 2024, las organizaciones en el país experimentaron un promedio de 3,124 ataques semanales, lo que representa un aumento interanual del 78%, de acuerdo con el Reporte Trimestral de Ataques de Checkpoint.

Como ya se ha compartido, todas las organizaciones y usuarios están expuestos a ataques cibernéticos, por lo cual los PACs (Proveedores Autorizados de Certificación) en México no están exentos debido a la dependencia de las tecnologías de la información y la comunicación para el manejo de información sensible, transacciones y operaciones tecnológicas y financieras.

A continuación, se detallan algunos de los principales riesgos cibernéticos que pueden afectar la operación:

1. Ataques de Ransomware

- **Descripción:** Los cibercriminales pueden cifrar los datos críticos del sistema y exigir un rescate para liberar la información. En este caso específico podría ser información confidencial de clientes o datos financieros, transacciones.
- **Impacto:** Posible interrupción de los servicios, pérdida de datos esenciales para la operación y daños a la confianza del cliente.

2. Phishing y Spear Phishing

- **Descripción:** Los atacantes intentan obtener acceso a información confidencial mediante correos electrónicos fraudulentos, suplantando identidades de confianza.
- **Impacto:** Robo de credenciales, acceso no autorizado a sistemas financieros o tecnológicos, posible manipulación de fondos o datos de clientes.

3. Ataques de Denegación de Servicio (DDoS)

- **Descripción:** Un ataque que busca saturar los sistemas y redes de la infraestructura crítica para interrumpir el acceso a los servicios.
- **Impacto:** Parálisis temporal de los servicios y afectación a la reputación de la entidad.

4. Acceso no autorizado a sistemas y bases de datos

- **Descripción:** Los atacantes pueden buscar vulnerabilidades en el software para obtener acceso no autorizado a sistemas críticos, además de información.
- **Impacto:** Exposición de información sensible, violación de la privacidad de los clientes y riesgo de fraude financieros.

5. Vulnerabilidades en el software o hardwares

- **Descripción:** Las fallas de seguridad en el software o hardware utilizado en la infraestructura pueden ser explotadas por atacantes.

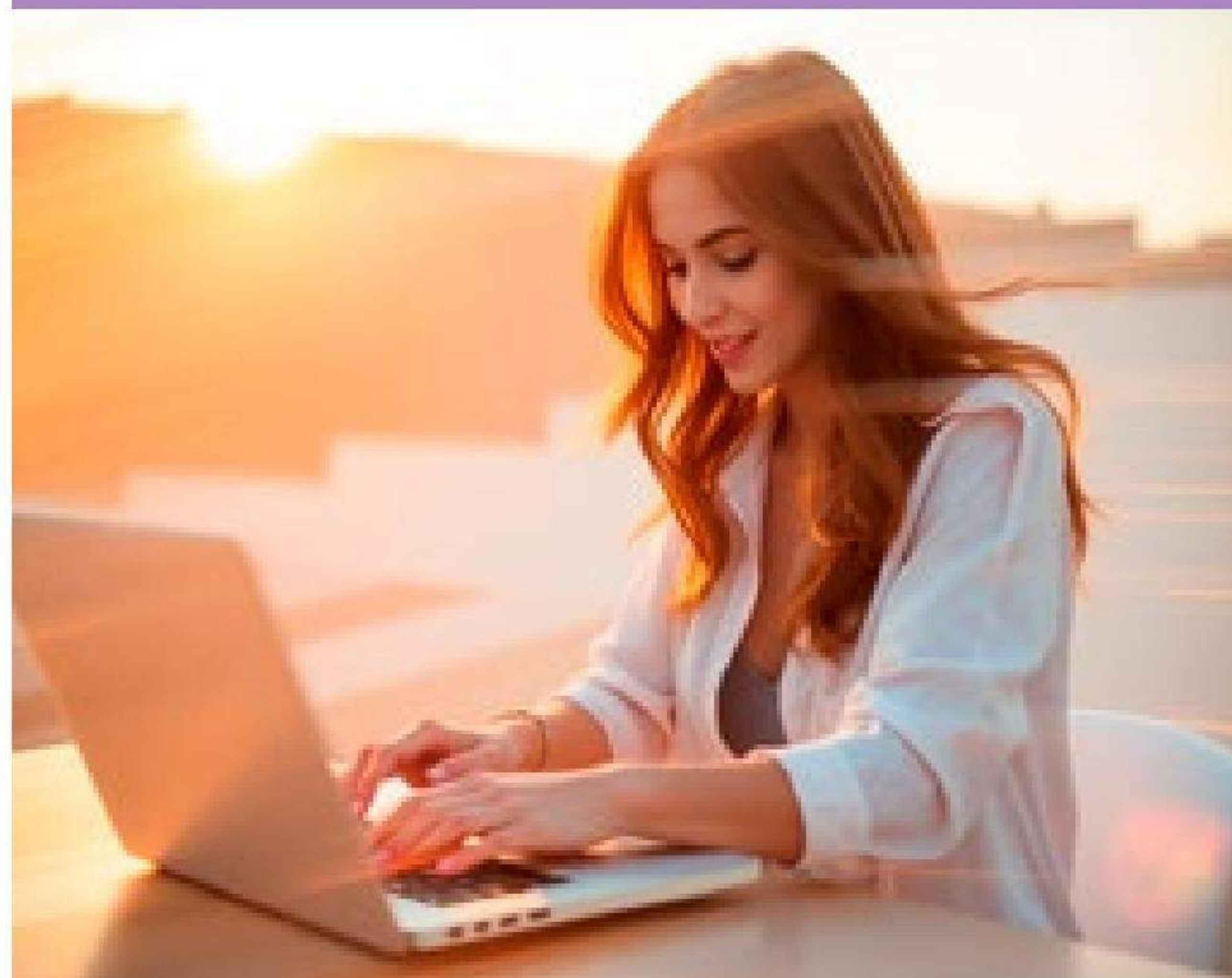
- **Impacto:** Exposición de la red a intrusos, pérdida de datos críticos y comprometimiento de los servicios tecnológicos y/o financieros.

6. Interrupciones en la cadena de suministro de TI

- **Descripción:** Dependencia de terceros para el suministro de software, hardware o servicios en la nube puede generar riesgos si estos proveedores sufren incidentes de seguridad.
- **Impacto:** Inestabilidad en los servicios críticos y posibles filtraciones de datos a través de proveedores comprometidos.

7. Malware y software malicioso

- **Descripción:** Programas dañinos como virus, troyanos y spyware pueden ser introducidos en los sistemas mediante dispositivos infectados o enlaces maliciosos.
- **Impacto:** Corrupción de datos, robo de información y afectación a la integridad de las transacciones tecnológicas o financieras.



8. Exposición a incidentes de privacidad y protección de datos

- **Descripción:** La pérdida de datos personales o financieros debido a brechas de seguridad puede afectar la confidencialidad de los clientes y usuarios.
- **Impacto:** Sanciones legales, pérdida de confianza por parte de los clientes y daño a la reputación corporativa.

9. Errores humanos o negligencia interna

- **Descripción:** Los empleados de la organización pueden ser responsables de divulgar información confidencial o de no seguir las políticas de seguridad adecuadas.
- **Impacto:** Acceso no autorizado a datos, implementación incorrecta de medidas de seguridad o fallos operativos.

10. Ataques a la infraestructura de comunicaciones

- **Descripción:** Las redes de comunicación utilizadas para realizar transacciones y operaciones pueden ser objeto de ataques como la interceptación de comunicaciones o ataques man-in-the-middle.
- **Impacto:** Manipulación de transacciones tecnológicas o financieras, robo de datos sensibles y afectación de la integridad de los servicios.





11. Falta de actualización o parcheo de sistemas

- **Descripción:** El uso de sistemas o aplicaciones desactualizadas con vulnerabilidades conocidas puede dejar la infraestructura susceptible a ataques.
- **Impacto:** Acceso no autorizado, explotación de vulnerabilidades conocidas y compromisos de la seguridad.

En conclusión:

Debido a que los PACs manejan información confidencial y sensible de clientes (contribuyentes), proveedores y terceros, además de regirse por los requerimientos y sanciones definidos por el Servicio de Administración Tributaria es de suma importancia contar con medidas, protocolos de seguridad tecnológica y capacitación continua del personal para evitar ciberataques, minimizar riesgos, fatalidades e impacto de negocio. Toda organización debe contar con una política integral de ciberseguridad, protección y segmentación de redes, cifrado de la información, privilegios de usuarios restringidos hasta un monitoreo 24/7 de la operación e intentos de ataque.



Amexipac celebra su 19ª Asamblea General Ordinaria

El pasado 5 de diciembre de 2024, los socios de Amexipac, integrada por los Proveedores Autorizados de Certificación (PACs), se dieron cita para llevar a cabo la 19ª Asamblea General Ordinaria.

Durante la reunión, se presentó el informe de actividades correspondientes al ejercicio 2024, destacando los logros y avances de la asociación en temas clave como la promoción de la facturación electrónica, la representación de los PAC ante las autoridades fiscales y la generación de conocimiento en el sector.

“La asamblea es un espacio clave para consolidar el compromiso de los socios con los objetivos de Amexipac y definir el rumbo de nuestras acciones futuras,” comentó un representante de la asociación.





Además de la revisión del trabajo realizado, se formalizó el proyecto de actividades para el 2025, que incluye iniciativas destinadas a fortalecer la presencia de los PAC, fomentar la capacitación de sus miembros y estrechar la colaboración con las autoridades fiscales y otros actores relevantes.

La participación activa de los socios fue clave para asegurar que las decisiones tomadas reflejen las necesidades y aspiraciones del gremio, reafirmando a Amexipac como un referente en la transformación digital fiscal en México.

Con esta asamblea, Amexipac cierra un año de retos y logros, mientras se prepara para consolidar su liderazgo en 2025.

Reconocimiento al esfuerzo: Premios Valor 2024

En diciembre de 2024, Amexipac llevó a cabo las votaciones para reconocer a los miembros más destacados y participativos dentro de los Comités Regulatorio y Técnico. Estos premios, conocidos como los Premios Valor, destacan la dedicación y las valiosas contribuciones realizadas por los integrantes a lo largo del año.

En la edición 2024, los ganadores fueron:

Comité Regulatorio:

- Yoshio Carrillo, de Comercio Digital.
- Emilio Bernal, de Interfactura.

Comité Técnico:

- Julio César Hernández, de Ateb.
- Alfredo Carrillo, de Quadrum.

Amexipac extiende sus más sinceras felicitaciones a los galardonados por su compromiso, esfuerzo y valiosa participación. Sus aportaciones han sido clave para resolver dudas y enfrentar los desafíos planteados por nuestros socios, fortaleciendo así el trabajo colectivo de cada comité.

“El compromiso de estos líderes refleja la esencia de Amexipac: sumar esfuerzos para impulsar la tributación digital en México.”

Este reconocimiento subraya la importancia de la colaboración activa y reafirma el compromiso de Amexipac con la excelencia y el trabajo en equipo. **¡Felicidades a los ganadores!**

Iniciamos el calendario de actividades Amexipac 2025

Amexipac arranca con entusiasmo el calendario de actividades 2025, diseñadas para fortalecer la capacitación, el cumplimiento normativo y la interacción con las autoridades fiscales. Durante enero, se marca el inicio de este año con una convivencia presencial con el SAT, que busca estrechar la relación y alinear objetivos con el organismo regulador.

El calendario también incluye actividades clave para los socios y agremiados:

- Convivencia presencial con el SAT: enero.
- Curso de Oficial de Cumplimiento Regulatorio: mayo.
- Curso de Oficial de Cumplimiento Tecnológico: agosto.
- Temas selectos: sesiones trimestrales en enero, marzo, junio y octubre.

Entre todas las actividades, destaca la 7ª edición del curso de acreditación para Oficial de Cumplimiento Regulatorio, una iniciativa fundamental para preparar a los Oficiales de Cumplimiento Regulatorio, quienes desempeñan un rol clave dentro de los Proveedores Certificados de Comprobantes Fiscales Digitales por Internet (conocidos como PAC).

Este curso permitirá:

- Actualizar y adquirir conocimientos sobre normatividad, operación y requisitos obligatorios para los PAC.
- Tomar medidas preventivas de cumplimiento normativo.
- Contribuir a que los socios mantengan su autorización otorgada por el SAT.

Amexipac reafirma su compromiso de brindar herramientas y espacios de formación que garanticen el cumplimiento y el liderazgo de los agremiados en el ámbito de la facturación electrónica.



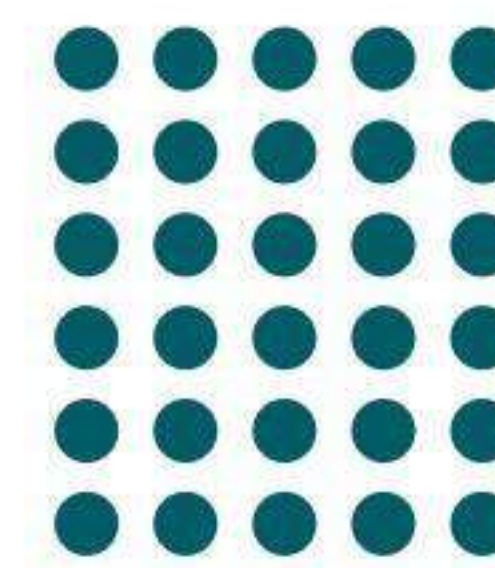
#SomosAmexipac
e impulsamos la tributación digital



**¡Prepárate para un año lleno de aprendizaje y colaboración!
Si aún no eres Socio AMEXIPAC,
¡afílate y participa!**

www.amexipac.org.mx

Plan Maestro del SAT



Martha Soria Castro



El Servicio de Administración Tributaria (SAT) dio a conocer el Plan Maestro 2025 el cual establece las acciones para alcanzar la meta de recaudación de 5.3 billones de pesos planteada para este año, sin crear ni aumentar impuestos, además de promover una cultura cívica contributiva.

El plan se basa en tres ejes fundamentales: atención al contribuyente, acompañamiento al contribuyente cumplido y fiscalización contra la evasión y el contrabando.

En el rubro de atención al contribuyente se encuentran:

- Simplificación de trámites y servicios, con el cual busca reducir los requisitos en los trámites de mayor demanda.
- Presencia del SAT en la República Mexicana,

con ello el SAT dará un mejor servicio al contribuyente a través de las 161 oficinas en las 32 entidades del país, además del uso de su oficina móvil.

- Nuevas facilidades para el Régimen Simplificado de Confianza (Resico)
- Renovación del Portal del SAT, para facilitar el acceso a los trámites y servicios.
- Potenciar el uso de las aplicaciones móviles, como son SAT Móvil y Factura SAT Móvil.
- Fomentar la cultura contributiva.

En acompañamiento al contribuyente el SAT contempla:

- Programa de Regularización Fiscal para pequeños contribuyentes. Durante 2025, las y los contribuyentes con ingresos de hasta 35 millones de pesos podrán corregir sus adeudos con reducción de 100% sobre recargos, multas y gastos de ejecución.
- Prellenado de declaraciones, habilitado para sector primario, Régimen de Coordinados y Régimen Opcional de Grupo de Sociedades.
- Actualización de la plataforma de declaraciones informativas, donde se podrán presentar en línea, la Declaración Informativa Múltiple, Declaración Informativa de Operaciones con Terceros, Multi-IEPS, entre otras.

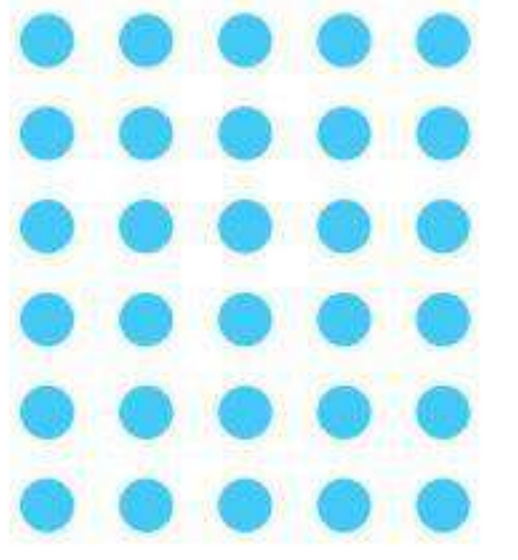
Como tercer rubro se muestra la fiscalización contra la evasión y el contrabando donde se incluye

- Continuar con el uso de herramientas tecnológicas para vigilar y garantizar el cumplimiento de las obligaciones tributarias y la detección de irregularidades.
- Intercambio de información y coordinación con otras autoridades federales como UIF, IMSS, STPS, Infonavit, entre otras.
- Revisión a sectores económicos que han mostrado alto riesgo de evasión, y fiscalización de los principales conceptos de planeaciones a través de sus esquemas reportables.
- Operativos de combate al contrabando y fiscalización profunda de las operaciones y participantes del comercio exterior.
- Mantener las acciones de litigio estratégico en tribunales federales para todos los asuntos.
- Participar con la Fiscalía General de la República en el fortalecimiento de los asuntos relacionados con los delitos de defraudación fiscal, contrabando, emisión y utilización de comprobantes falsos, para conseguir la vinculación a proceso de personas físicas y morales, así como la solicitud de providencias precautorias para garantizar el interés fiscal.
- Continuar publicando en el Diario Oficial de la Federación reglas, criterios normativos y criterios no vinculativos para atacar las prácticas fiscales agresivas en materia de evasión y contrabando.
- Fortalecer los procesos de capacitación y supervisión para continuar avanzando en la profesionalización de funcionarios y el combate a la corrupción.

Con el Plan Maestro 2025, se fortalece la recaudación fiscal, sin privilegios del pasado y poniendo la tecnología al servicio de la gente y de la nación, en beneficio de las finanzas públicas de México.



Hecho en México: El sello que impulsa la identidad y competitividad de los productos mexicanos



Anyel Carrillo de Albornoz



En el dinámico mundo del comercio internacional, los productos que llevan el distintivo **"Hecho en México"** no sólo representan calidad e innovación, sino

también el orgullo y el esfuerzo de miles de mexicanos. Este emblema, reconocido en mercados nacionales e internacionales, se ha convertido en un símbolo de competitividad y confianza.

Recientemente, en la presentación del Plan México, la Presidenta Claudia Sheinbaum, dio a conocer se está desarrollando el Plan Nacional de Desarrollo para los próximos seis años y uno de los puntos de la misión del Plan es justamente el relanzamiento del programa "Hecho en México", por ello es importante conocer qué es este distintivo.

¿Qué es el distintivo "Hecho en México?"

Es un sello oficial que identifica los bienes producidos en territorio mexicano. Su objetivo

es claro: permitir que los consumidores, tanto locales como internacionales, reconozcan estos productos como genuinamente mexicanos, respaldados por su origen y calidad.

¿Para qué fue creado?

El distintivo tiene múltiples propósitos, todos orientados a fortalecer la economía mexicana:

- Impulsar el mercado interno.
- Posicionar los productos mexicanos en el ámbito internacional.
- Proteger el empleo en México.
- Incrementar la competitividad de los productos fabricados en el país.

¿Cómo obtener el distintivo?

El proceso se gestiona a través del **Sistema Integral de Normas y Evaluación de la Conformidad (SINEC)**, desarrollado por la Secretaría de Economía. Los interesados, ya sean personas físicas o morales, deben seguir estos pasos básicos:

- **Acceder al portal:** www.sinec.gob.mx.
- **Completar el formulario:** Ingresar usuario y contraseña, y llenar la solicitud con la información requerida.
- **Subir la documentación necesaria:**
- **Para personas morales:** RFC, acta constitutiva e instrumento que acredite al representante legal.
- **Para personas físicas:** RFC y escrito libre de solicitud.
- **Acreditación vigente:** Presentar un documento emitido por la Entidad Mexicana de Acreditación (EMA).

El rol de los organismos de certificación

El distintivo “Hecho en México” se otorga únicamente a través de organismos de certificación autorizados por la Dirección General de Normas (DGN) y acreditados por la EMA. Estos organismos verifican que los productos cumplan con los criterios de valor agregado nacional, calidad, innovación, diseño, sustentabilidad e inclusión laboral.

Para ser elegible, los bienes deben cumplir con al menos uno de los siguientes requisitos:

- Ser producidos totalmente en México.
- Utilizar materiales originarios conforme a tratados comerciales vigentes.



- Someterse a un proceso de producción que transforme los bienes no originarios en productos clasificados en una subpartida diferente según el Sistema Armonizado de Codificación.

Duración y renovación del distintivo

El uso del emblema “Hecho en México” tiene una vigencia inicial de dos años, con la posibilidad de renovarse por el mismo periodo. Durante este tiempo, los usuarios deben cumplir con las especificaciones contenidas en el **Manual de Identidad Gráfica**, disponible en el SINEC.

¿Por qué es importante este distintivo?

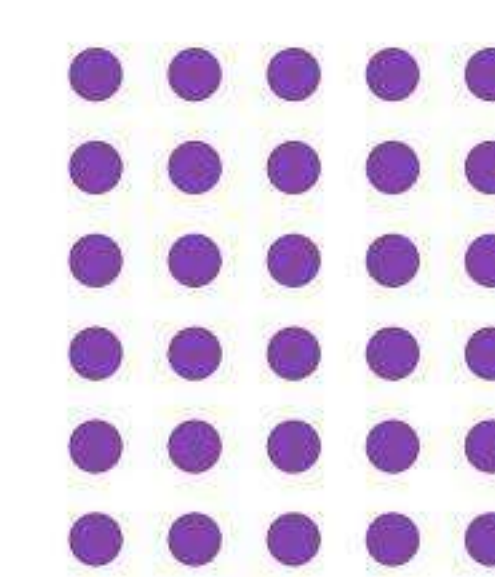
El emblema no solo resalta la calidad de los productos mexicanos, sino que también protege su identidad en mercados internacionales. Es una herramienta clave para generar confianza entre consumidores y socios comerciales, fomentando la preferencia por lo hecho en México.

“El distintivo ‘Hecho en México’ no es solo un sello, es un reconocimiento al trabajo, la creatividad y la innovación que caracterizan a nuestro país.”

Si eres productor mexicano y buscas posicionarte en mercados nacionales e internacionales, este distintivo puede marcar la diferencia. Ingresa a www.sinec.gob.mx y descubre cómo obtenerlo. ¡El mundo está listo para reconocer la calidad mexicana!



¿Cuál será el futuro de la Inteligencia Artificial en las Administraciones Tributarias?*



Alfredo Collosa



A veces se dice que la mejor forma de predecir el futuro es conociendo el pasado y el presente. En materia de nuevas tecnologías y en especial cuando se trata de Inteligencia Artificial (IA) la respuesta no es tan sencilla y menos aún cuando se trata de predecir su uso y aplicación en las Administraciones Tributarias (AATT).

Vaya como prueba la aparición el 30 de noviembre 2022 de Chat GPT de la empresa OpenAI el cual marca un antes y un después en la materia.

Hasta esa fecha conocíamos la “IA predictiva”, que analiza los datos para ofrecer recomendaciones, previsiones y perspectivas, pero con Chat GPT surgió la “IA generativa”, como aquella que aprende de los datos y utiliza patrones para generar texto, imágenes, música y código sin problemas.

Es evidente que el uso de la IA presenta múltiples beneficios para las AATT entre las que se destacan la mejora en el manejo de la información, analizar el comportamiento de datos, mejorar los servicios a los ciudadanos, optimizar los procesos, reducción de costos, por nombrar solo algunos.

La IA también tiene la capacidad de facilitar la detección de correlaciones previamente indetectables u ocultas, actividad sospechosa, tendencias, indicadores, etc., lo que podría permitir la detección temprana y la acción preventiva, o la mitigación de estos riesgos en tiempo real, lo que ayudaría a reducir la brecha fiscal y aumentar la recaudación de impuestos.

Por tal motivo la IA se está expandiendo a pasos agigantados en las distintas funciones de las AATT considerando la inmensa capacidad de datos que disponen y el aumento del poder de cómputo con el consiguiente avance de nuevas tecnologías como la IA generativa comentada.

También hay que destacar que el uso de la IA presenta riesgos entre los que se destacan los sesgos de distinto tipo, uso injustificado de los datos de los ciudadanos con vulneración de la privacidad de los datos personales, utilización de sistemas de IA no transparentes, falta de rendición de cuentas, en definitiva, una inadecuada protección de los derechos y garantías de los contribuyentes.

Frente a ello han surgido diversas iniciativas o marcos regulatorios para que la IA se utilice siempre en beneficio de los ciudadanos de una manera ética y responsable, entre las que se destacan la Ley de la UE de la IA, los principios de IA de la OCDE, Directrices éticas para una IA fiable de la UE, el Acuerdo mundial de la ética de la IA de la UNESCO, así como múltiples leyes de los países que se están aprobando.

Respecto a las tendencias en el uso de la IA en las AATT interesa destacar que ya en El informe “Tax Administration 2023” de la Serie de Administración Tributaria de la OCDE [1] se dijo que más del 60% de las AATT ofrecen asistentes virtuales o digitales para ayudar a responder las consultas de los contribuyentes y respaldar el autoservicio, un cambio de casi 30 puntos porcentuales en comparación con 2018.

Cerca del 95% de las AATT informan que utilizan ciencia de datos y herramientas analíticas para manipular datos electrónicos de terceros, incluidas otras AATT, así como datos electrónicos generados internamente para guiar su trabajo de cumplimiento. Se trata de un aumento de más de 20 % en comparación con 2018.

Adicionalmente, el 54,4 por ciento de las AATT están utilizando IA y machine learning en su gestión tributaria, y el 50 % aplicado la automatización robótica de procesos, con incrementos de más del 22 % de 2018 a 2021.

En otra parte del documento de 2023 se dice que “Más del 80% de las AATT informan que están utilizando o que están en la fase de implementación para el uso futuro de técnicas de vanguardia para explotar datos de manera que reduzcan la necesidad de intervención humana.

Por su parte en la reciente publicación Tax Administration 2024 [2] destaca que se sigue avanzando con el uso de la IA al decir que las AATT han empleado innovaciones tecnológicas durante años y el número de AATT que utilizan asistentes virtuales, IA e interfaces de programación de aplicaciones continúa aumentando.

Por ejemplo, entre las AATT cubiertas por la publicación, la adopción del uso de asistentes virtuales e IA casi se ha duplicado desde 2018.

Así mismo, dice que el uso de la IA, incluido el aprendizaje automático, para la evaluación de riesgos y la detección de fraudes ya lo utilizan o están en proceso de implementarse en aproximadamente la mitad de las AATT cubiertas en la publicación.

Se afirma que este uso cada vez más sofisticado de la analítica en conjuntos de datos ampliados está dando lugar a una mejora de la gestión de riesgos y al desarrollo de una serie de medidas de intervención, incluso mediante procesos automatizados.

Así mismo el Instituto de Estudios Fiscales (IFS), instituto de investigación económica independiente del Reino Unido, publicó un muy interesante informe titulado en inglés “Artificial intelligence in automated decision-making in tax administration: the case for legal, justiciable and enforceable safeguards” [3] el cual se centra en el uso de la IA en la gestión administrativa en las AATT para tomar decisiones discrecionales o subjetivas.



El informe si bien se basa en la utilización de la IA para toma de decisiones automatizadas en la AT del Reino Unido que es el HMRC, entiendo es de suma utilidad para



todas las AT y partes interesadas en el tema.

En el marco operativo actual, en general, en lo que respecta a las decisiones tomadas

por la HMRC (en particular, las decisiones discrecionales), los funcionarios de la HMRC son los principales encargados de la toma de decisiones, aunque puedan contar con la ayuda de la tecnología para tomarlas.

Sin embargo, una vez que se implemente la IA en la gestión de la AT, cuando una decisión se tome únicamente mediante IA (en particular, aprendizaje automático (ML) sin intervención humana en el proceso de toma de decisiones), esto reflejaría una decisión tomada por el sistema (y no una decisión de un funcionario de la HMRC); la decisión tomada por la IA se basaría en la propia interpretación del modelo de los datos (ya sea etiquetados o no) y las correlaciones extraídas por el modelo.

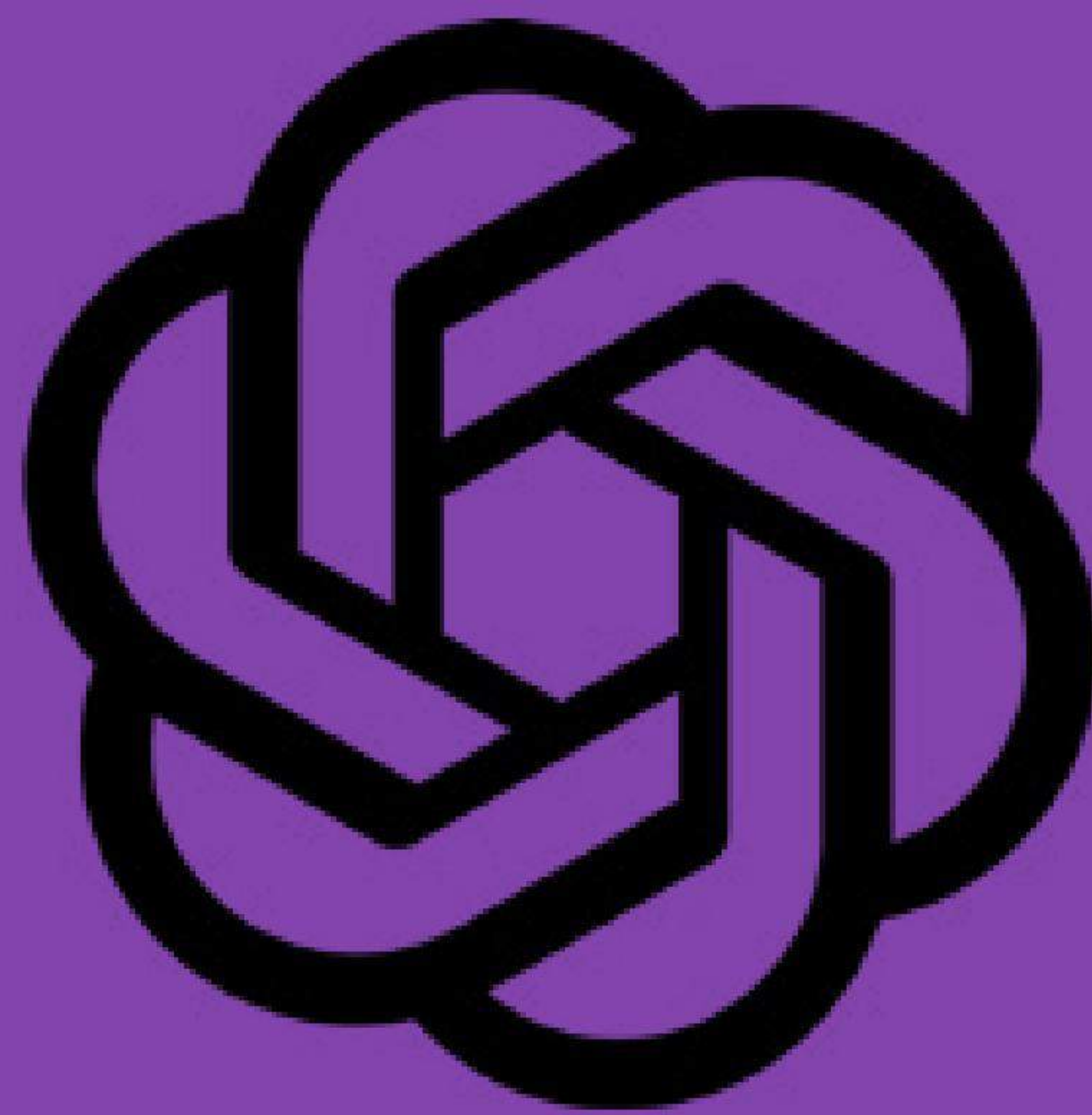
Esto reflejaría un cambio en el papel del principal encargado de la toma de decisiones, del funcionario de la HMRC a la IA.

Incluso cuando se requiere que un funcionario de HMRC revise una decisión tomada por la IA antes de que la decisión tenga un impacto en un contribuyente y el funcionario de HMRC proporcione una explicación de por qué se llegó a esa decisión, cuando se utiliza una IA de caja negra, esa explicación se basa únicamente en la comprensión del funcionario de por qué se llegó a una decisión en particular debido a la opacidad de la IA de caja negra.

La explicación del funcionario de HMRC implicaría aplicar ingeniería inversa a la lógica y la base de la decisión generada por la IA, y esta ingeniería inversa inculca un elemento de incertidumbre y falta de fiabilidad en las explicaciones proporcionadas por el funcionario de HMRC.

Por ello el informe recomienda un enfoque proactivo para regular el uso de la IA en la gestión de la AT, en lugar de un enfoque reactivo, especialmente teniendo en cuenta algunos de los riesgos (que se han manifestado en varias jurisdicciones que ya han adoptado la IA en la administración pública).

En el documento se recomiendan dos soluciones alternativas: una legislación sobre IA



específica para los impuestos o una Carta de IA de la HMRC (que incluya algunos de los estándares y valores clave que la HMRC debe respetar) (en conjunto, ambas medidas se denominan «Garantías legales fiscales para la IA»).

En definitiva, respecto al interrogante que me motivó a escribir este blog ¿Cuál será el futuro de la IA en las AATT? Creo que si bien hay incertidumbre respecto a cómo avanzará la tecnología por un lado y los marcos regulatorios por el otro creo que la IA se expandirá aún más en las AATT en todas sus funciones, aún en otras que hoy no se utiliza.

Por citar un ejemplo los asistentes virtuales que hoy se utilizan para información y asistencia podrán utilizarse para recursos humanos en la selección y reclutamiento de personal al igual que ya se hace unas muchas empresas del sector privado, como así también para apoyar a los auditores en su trabajo y porque no para intercambiar información fiscal dentro de los países entre distintos organismos como así mismo internacionalmente.

Así mismo los funcionarios de las AATT cada vez más utilizarán asistentes ba-

OpenAI

sados en IA para sus tareas cotidianas y por qué no pensar que existan “funcionarios con IA” que puedan realizar tareas de forma independiente, tomar decisiones e incluso interactuar con otros funcionarios.

Si tuviera que predecir de que factores dependerá el futuro de la IA en las AATT diría que habría que analizar varios factores como los avances en la IA, por ejemplo, que IA vendrá luego de la IA Generativa.

Así mismo un factor clave será el avance de los marcos normativos en cada uno de los países donde las AATT ejercen sus funciones.

Finalmente, las resoluciones de la justicia en la materia entiendo serán un tema vital ya que en cada caso concreto de uso de la IA por parte de las AATT los organismos jurisdiccionales tendrán que decir si se han vulnerado o no derechos de los ciudadanos.

Lo que si estoy convencido es que las AATT nunca deben perder de vista que la tecnología como la IA es una herramienta

y no un objetivo en sí mismo, vale decir que sólo deberían incorporarla cuando las ventajas superen a las desventajas y en definitiva solucionen los problemas que se presentan y sirvan para ser más eficientes y eficaces en su cometido.

Pero en todo ello será siempre vital usar la IA de manera ética y responsable es decir buscando no vulnerar los derechos y garantías de los ciudadanos.

¿Ustedes que opinan del tema?

[1] OECD (2023), Tax Administration 2023: Comparative Information on OECD and other Advanced and Emerging Economies, OECD Publishing, Paris, <https://doi.org/10.1787/900b6382-en>.

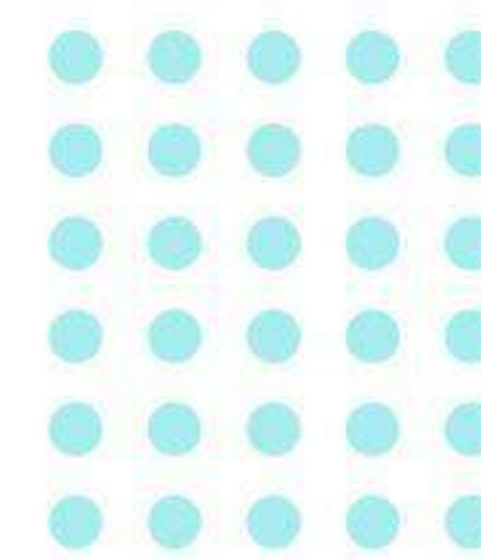
[2] OECD (2024), Tax Administration 2024: Comparative Information on OECD and other Advanced and Emerging Economies, OECD Publishing, Paris, <https://doi.org/10.1787/2d5f-ba9c-en>.

[3] Nathwani, K. (2024). *Artificial intelligence in automated decision-making in tax administration: the case for legal, justiciable and enforceable safeguards*. London: Institute for Fiscal Studies. Available at: <https://ifs.org.uk/publications/artificial-intelligence-automated-decision-making-tax-administration-case-legal> (accessed: 12 September 2024).

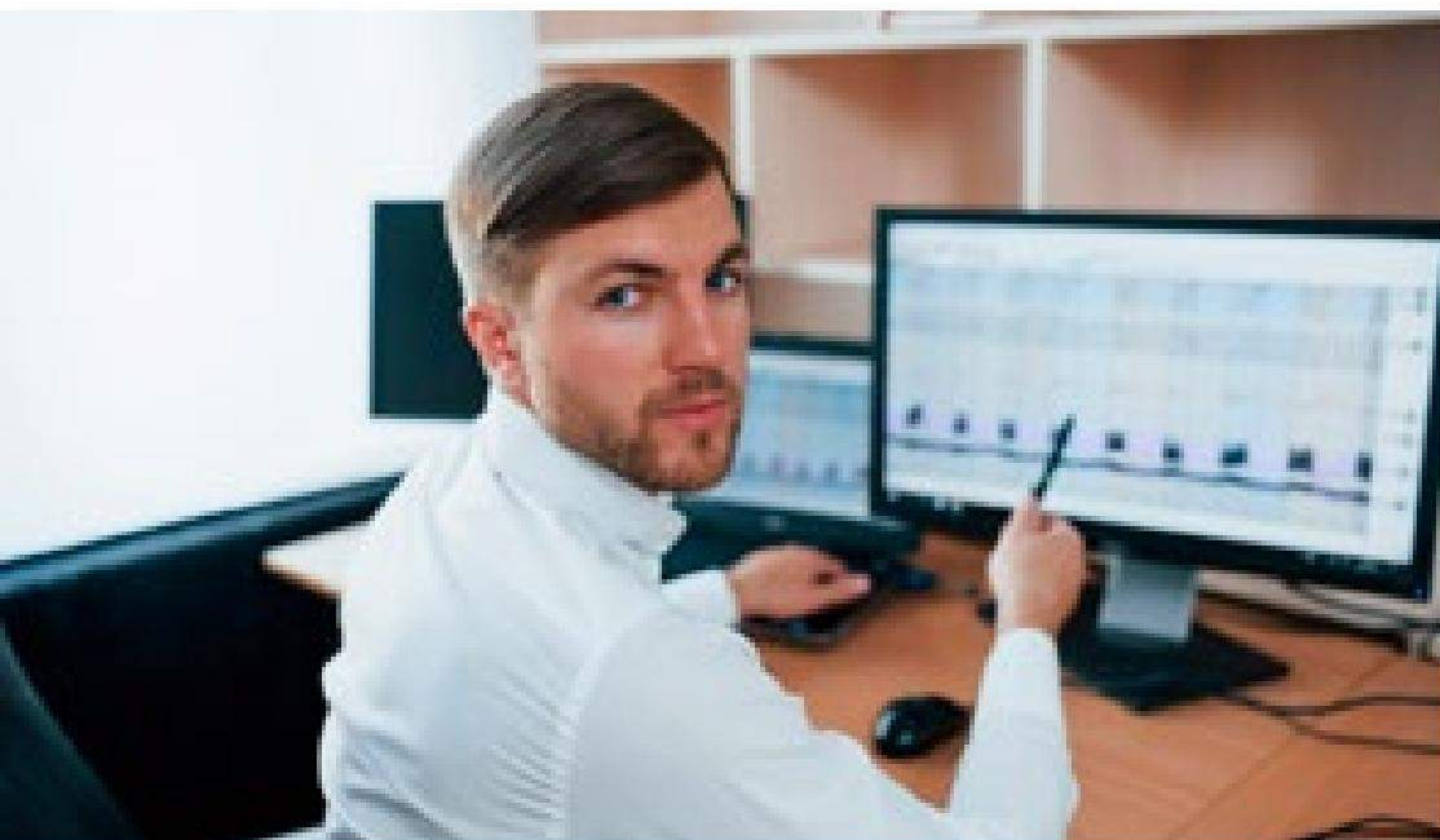
* Artículo publicado originalmente en el sitio de internet del Centro Interamericano de Administraciones Tributarias: <https://www.ciat.org/ciatblog-cual-sera-el-futuro-de-la-inteligencia-artificial-en-las-administraciones-tributarias/>



Detección del lavado de dinero con ayuda de la IA



Genaro Eliseo Gómez Muñoz



El acelerado avance tecnológico como la aparición de la Inteligencia Artificial (IA) que, con volúmenes cada vez mayores de datos y procesos de supervisión relacionados, ha transformado y trastornado nuestras vidas de manera increíble, y la dinámica de las actividades requiere cambios sustanciales.

El ritmo de la innovación que genera nuevas amenazas y la creciente complejidad de los delitos financieros, así como los marcos regulatorios globales están creando un entorno cada vez más desafiante para las instituciones financieras y las no financieras. De acuerdo con la Organización para la Cooperación y el Desarrollo Económicos (OCDE) se define a la IA como un sistema basado en una máquina que, dado un conjunto de objetivos definidos por el ser humano, puede hacer predicciones, recomendaciones o tomar decisiones que influyen en el entorno real o virtual. Los sistemas de IA, diseñados para funcionar con distintos niveles de autonomía, implican la introducción de

grandes cantidades de datos relevantes para una tarea concreta y la creación de un conjunto de reglas que ayuden a la máquina a aprender de esos datos para determinar cómo realizar eficientemente la tarea.

La filosofía central del sistema de IA

Se refiere a utilizar algoritmos para identificar patrones sub-yacentes generalmente ocultos a simple vista. Estas acciones imitan al cerebro humano, lo que implica cierto grado de pensamiento, análisis, razonamiento y discreción.

Cuando estas acciones las realiza una máquina, se dice que son artificialmente inteligentes. Algunos ejemplos, que ya vemos en nuestros días y que cada vez nos sorprenden más, son la tecnología de reconocimiento facial (Deep Fake) y de voz, los robots que actúan con la apariencia de humanos, los automóviles autónomos sin conductor o los drones que entregan paquetería o comida a domicilio; avances tecnológicos sorprendentes.

Ahora bien, el ecosistema antilavado de dinero mundial se encuentra adoptando estas herramientas para detectar las miles de transacciones fraudulentas. Las instituciones financieras en el mundo enfrentan retos crecientes para identificar y detener los flujos de dinero ilícito en tiempo real, resultando en pérdidas financieras y riesgos de cumplimiento, y es que la delincuencia

organizada utiliza cada vez nuevos métodos de lavado de dinero. El informe global sobre delitos financieros 2024, elaborado por el Nasdaq, menciona que un estimado de 3.1 billones de dólares en fondos ilícitos fluyeron por medio del sistema financiero mundial en 2023.

El lavado de dinero representó billones de dólares para financiar una variedad de delitos destructivos, incluidos aproximadamente 346.700 millones de dólares en trata de personas y 782.900 millones de dólares en actividades de tráfico de drogas, así como 11.500 millones de dólares en financiación del terrorismo. En 2023, las estafas y los esquemas de fraude bancario totalizaron 485.600 millones de dólares en pérdidas proyectadas a escala mundial.

Con cifras tan alarmantes que nos presenta este informe y la creciente preocupación de la comunidad internacional en el ámbito del lavado de dinero, el sistema financiero global se encuentra adoptando herramientas de IA para detectar las operaciones y transacciones fraudulentas. El fraude también ha evolucionado con el uso de IA, por lo que se ha incrementado la complejidad para que las entidades financieras puedan detectar redes de movimientos transaccionales fraudulentos y el uso de identificaciones falsas, suplantación de identidad además de los movimientos y clientes reales.

Uno de los dolores de cabeza que a escala global traen al sistema financiero trabajando en ello es la tipología de las “mulas bancarias” que representan un gran problema, en la mayoría de los casos las personas que no saben que se está haciendo algo ilegal —y miren que el perfil de ellos adultos mayores y jóvenes universitarios se encuentran entre los más vulnerables—. Con la implementación

de IA se pueden entender grandes cantidades de datos y correlacionarlos, y así detectar el tipo de comportamientos de estas personas llamadas “mulas bancarias” para alertar a los bancos y tomar acciones al respecto. Por ejemplo, transacciones de clientes del banco que son monitoreadas y que con esa información se crean los modelos estadísticos que mediante IA pueden detectar un potencial fraude o actividad atípica.

Por lo difícil que resulta identificar si es una transacción atípica, es clave analizar esos movimientos anormales, los montos, horarios de las transacciones, lugar geográfico, etcétera.

Conclusión:

Como se puede apreciar, la IA ayuda significativamente a realizar el trabajo de supervisión utilizando los recursos disponibles para producir resultados de alta calidad. Por medio de diversos análisis, las herramientas de IA identifican patrones y excepciones para su posterior investigación por la parte humana, pues cabe destacar que la IA no puede sustituir a los humanos para investigar más a fondo las condiciones, causas y efectos reales, todo ello para aumentar las posibilidades de mitigar acciones fraudulentas. De tal manera que es importante e imperativo que la IA se emplee como tecnología auxiliar para aumentar el proceso de profesionales o mano de obra cualificada para aprovechar la tecnología de IA. Utilizar la IA es alentador, por consiguiente, debemos prepararnos para afrontar los retos de la lucha frontal y tecnológica contra el lavado de dinero.

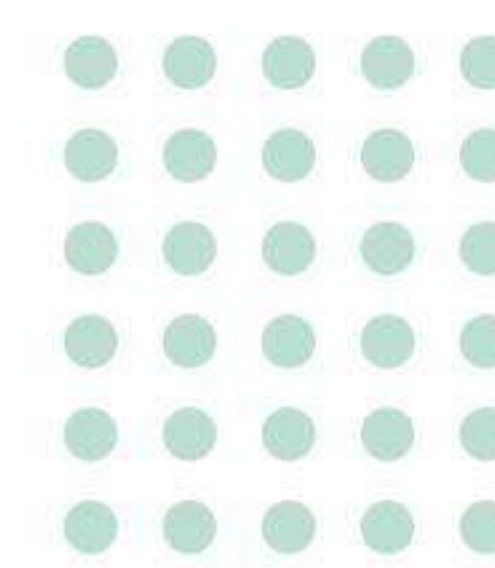
Fuentes consultadas

<https://www.nasdaq.com/global-financial-crime-report>
<https://www.eleconomista.com.mx/sectorfinanciero/Avanza-uso-de-Inteligencia-Artificial-para-detectar-lavado-de-dinero-20240625-0110.html>
www.oecd.org

Artículo publicado originalmente en la revista Contaduría Pública del IMCP.



Beneficios y Desafíos de los impuestos ecológicos en economías emergentes



Brenda Denisse Hernández Bravo



Introducción:

Los impuestos ecológicos, también conocidos como impuestos verdes, se implementan para incentivar prácticas sostenibles y reducir los impactos ambientales negativos.

En países en desarrollo, estos impuestos representan una herramienta valiosa para abordar problemas como la contaminación y el cambio climático, promoviendo la transición hacia economías más sostenibles. Sin embargo, su implementación enfrenta diversos desafíos relacionados con la capacidad administrativa, la aceptación social y los efectos económicos en sectores vulnerables.

El análisis de los beneficios y desafíos que enfrentan las economías emergentes presentan un gran reto debido a que la finalidad principal es:

1. Fomentan la sostenibilidad y reducción en la contaminación, ya que las empresas y personas que contaminan más pagan más impuestos.
2. Generan ingresos para los gobiernos que pueden utilizarse para proyectos ambientales y sociales.

Pese a que el principal objetivo de un gravamen verde es reducir el daño ambiental de alguna

actividad humana, este también puede ser un medio de recaudación que ayude a incrementar los ingresos de un gobierno.

La hipótesis del doble dividendo, planteada por Pearce, D. (1991), sirve para justificar un aumento en la recaudación por medio de una “reforma fiscal verde” por dos principales razones:

1. Efecto distorsionador dentro de la economía es menor comparado a otro tipo de impuestos.
2. Efecto compensatorio, puesto que es capaz de mejorar la eficiencia fiscal cuando su recaudación es utilizada para financiar reducciones en otros tributos distorsionantes (Rodríguez, M. 2001).



Sin embargo, la efectividad del impuesto verde puede reducirse si este no se aplica de manera correcta. Primero es necesario que se grave a la producción final, puesto que gravar a productos intermedios aumenta los costos.

En segundo lugar, el impuesto ambiental debe tener como principal propósito el reducir las externalidades negativas, puesto que, si se elabora con fines exclusivamente recaudatorios, entonces esta reducción podría verse afectada, dado que la tasa aplicada puede ser superior al costo marginal incurrido por la existencia de la externalidad (Hernández, C. y Urzua, C. 2023).

Para analizar la recaudación de los impuestos, a continuación, se muestra la eficiencia en la recaudación en México en el ejercicio 2023:



Cuadro 1: Recaudación por impuestos verdes subnacionales en 2023.

Entidad	Recaudación por impuesto verde (pesos per cápita)	Proporción como porcentaje de impuestos (%)	Proporción como porcentaje de ingresos (%)
Baja California	9.0	0.33	0.04
Campeche	2.9	0.17	0.01
Coahuila	12.3	0.87	0.06
Durango	39.7	2.45	0.19
Estado de México	4.7	0.35	0.02
Guanajuato	15.7	0.75	0.09
Nayarit	0.6	0.05	0.003
Nuevo León	261.6	8.62	1.09
Oaxaca	9.2	2.35	0.04
Querétaro	126.5	5.49	0.59
Quintana Roo	31.7	0.88	0.14
Yucatán	64.3	4.51	0.28
Zacatecas	205.9	18.86	0.95
Promedio	60.3	3.51	0.27

Fuentes: Elaborado por el CIEP, con información de: Leyes de Ingresos Estatales (2023).

Como dato informativo la recaudación por impuestos verdes en 2023 suma 2 mil 590.7 mdp. Esto representa, en promedio, el 3.5% de los ingresos percibidos por impuestos y 0.27% de los ingresos totales de las 13 entidades que los recaudan.

Para que este tipo de impuestos tengan un beneficio más directo, es deseable que, los ingresos obtenidos, estén “etiquetados” es decir, que los ingresos obtenidos se usen con un fin en particular; por ejemplo, el consumo de gasolina produce una externalidad negativa en el resto de la población en forma de aumentos en gastos de salud por la contaminación del aire, por lo tanto, sería deseable que, el ingreso obtenido por el Impuesto Especial Sobre Producción y Servicios (IEPS) a las gasolinas, sea destinado a conceptos como: atender la salud de pacientes con problemas respiratorios a causa de la contaminación, mejorar el transporte público (transporte sostenible), por mencionar algunos.

Desarrollo:

Los impuestos ecológicos se han convertido en herramientas clave para enfrentar las crecientes problemáticas ambientales derivadas del cambio climático y la contaminación.

En esencia, estos impuestos son mecanismos económicos diseñados para influir en el comportamiento de consumidores y productores, gravando las actividades que generan efectos negativos en el medio ambiente, como las emisiones de gases de efecto invernadero (GEI) o la contaminación de los recursos hídricos (Pizarro, 2021).

Existen diversas formas de impuestos ecológicos, los cuales pueden adaptarse a las necesidades y características de cada región:

1. Impuestos sobre emisiones: Estos gravan las emisiones de gases contaminantes, como el dióxido de carbono (CO₂) o el metano (CH₄). Son comunes en países con altos niveles de industrialización.

2. Impuestos sobre productos específicos: Incluyen gravámenes sobre productos como plásticos de un solo uso, pesticidas, o fertilizantes químicos.

3. Impuestos sobre la extracción de recursos: Estos se aplican a actividades como la minería, el uso de agua o la tala de bosques. En países con abundantes recursos naturales, como los de América Latina o África.

Actualmente, las empresas mexicanas deben estar preparadas para reportar sobre el desempeño ambiental bajo los estándares de las NIS (Normas internacionales de Sostenibilidad y los IBSO) ante las autoridades, pero también, a los usuarios externos, cadenas de valor y entidades financieras.

“Organizaciones y sociedad civil deben trabajar en conjunto para ser eficientes en sus procesos productivos, utilizar fuentes renovables, disminuir el consumo de energía y agua, etc.” (Zamora, 2023)





Para reconocer cuáles son los riesgos inherentes en la operaciones de las empresas se deben analizar los procesos y la información generada por la compañía, así como la información disponible en el sector y la industria de sus competidores; habrá que indicar las fuentes de donde se obtuvieron los datos o información para sustentar por qué se revelan esos riesgos; cuando no puedan cuantificarse los riesgos, se deben elaborar estimaciones que detallen y expliquen para informar al lector de los estados financieros de esta situación.

La administración debe asignar a una persona, equipo, área o consultor externo para la implementación de controles, procedimientos y para identificar los riesgos, así como emplear métricas (la norma los denomina IBSO) para determinar la gravedad e impacto de una acción. (Zamora, 2023)

Importante hay que destacar, que todo lo anterior referente a la evaluación ambiental, ayuda, efectivamente, a cumplir con las regulaciones ambientales, pero también, resulta en una gestión más eficiente de los recursos, una mejora en la reputación de la empresa, y una contribución positiva a la sostenibilidad a largo plazo en México; siempre y cuando, las empresas mexicanas hagan de este proceso una mejora continua y seguimiento puntual bajo los estándares establecidos.

Si aún no tienes claro cómo empezar a gestionar tus impactos asociados a cambio climático, agua o residuos peligrosos, coordinemos una reunión e identifiquemos en conjunto como tu empresa podría avanzar en torno al Impuesto Verde en México. (Proyecta Impacto, 2023).

Conclusión:

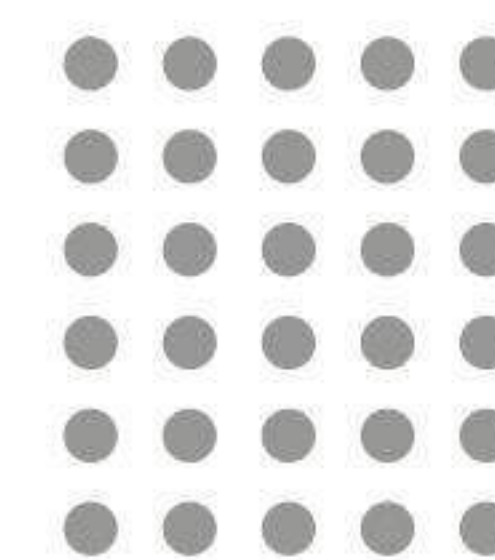
Los impuestos ambientales son una herramienta efectiva para reducir la contaminación y promover la sostenibilidad. Al establecer un costo económico para las actividades que dañan al medio ambiente, estos impuestos incentivan a empresas, personas, familias a adoptar prácticas más respetuosas con el medio ambiente, cabe mencionar que como se relató anteriormente tiene diversas ventajas y grandes desafíos para los implementadores (gobernantes).

Referencias:

- CINIF, 2023, Auscultación de las NIS 1 Y NIS 2, 2023, de CINIF: https://www.cinif.org.mx/uploads/Carta_Auscultacion_NIS-1_y_NIS-2.pdf
- (2022). Finanzas públicas locales: hacia una nueva coordinación fiscal: https://finanzaslocales.ciep.mx/FinanzasLocales_CIEP_29_06_22.pdf.
- (2023). Desarrollo sostenible: usos y recursos públicos: <https://desarrollosostenible.ciep.mx/wp-content/uploads/2023/03/ODS-usos-y-recursos.pdf>.
- [https://cadep.ufm.edu/concepto/externalidades/#:~:text=Las%20instancias%20donde%20las%20acciones,\(Stiglitz%201986%2C%2080\).](https://cadep.ufm.edu/concepto/externalidades/#:~:text=Las%20instancias%20donde%20las%20acciones,(Stiglitz%201986%2C%2080).)
- Externalidades y costos sociales: [https://cursos.clavijero.edu.mx/cursos/197_m/modulo4/contenidos/tema4.3.html#:~:text=El%20costo%20marginal%20social%20es,y%20el%20costo%20marginal%20externo.&text=Los%20costos%20se%20expresan%20en,representan%20un%20costo%20de%](https://cursos.clavijero.edu.mx/cursos/197_m/modulo4/contenidos/tema4.3.html#:~:text=El%20costo%20marginal%20social%20es,y%20el%20costo%20marginal%20externo.&text=Los%20costos%20se%20expresan%20en,representan%20un%20costo%20de%20)
- Artículo publicado originalmente en el boletín Visión Contable, del CCPGJ.



Ya no basta solo el CFDI



Emilio Ávila Muñoz



El comprobante fiscal es un factor determinante en la comprobación de las operaciones de los contribuyentes, que ha pasado de un comprobante impreso en papel a un comprobante fiscal digital (CFD), en el año de 2005, y que posteriormente evoluciona a un comprobante fiscal digital por internet (CFDI), obligatorio a partir del año 2014, este último derivado de la migración de los sistemas que la autoridad mantenía en sitio a una plataforma en internet.

El CFDI provee información relevante a la autoridad fiscal, lo que le ha permitido, con el uso de la tecnología, un efectivo combate a la elusión agresiva y a la evasión tributaria, priorizando la gestión tributaria (asistencia, control y vigilancia de obligaciones) sobre las facultades de comprobación (inspección, verificación, determinación y liquidación), con una rentabilidad de fiscalización de 201.6 pesos recuperados por cada peso invertido, de acuerdo con el informe tributario y de gestión del Servicio de Administración Tributaria (SAT), del primer trimestre de 2024.

La gestión tributaria se ha enfocado en detectar inconsistencias entre la información contenida en los CFDI y la información reportada en las declaraciones de los contribuyentes, como parte de un plan de fiscalización extensivo o masivo (vigilancia profunda). Sin embargo, se observan señales de que la fiscalización ya



no es suficiente con la vigilancia y control de obligaciones, ahora se ha empezado a exigir acreditar la materialidad de las operaciones y posteriormente determinar si el contribuyente cumple con los requisitos de indispensabilidad, los formales de ley, los anti elusivos y los antiabusos.



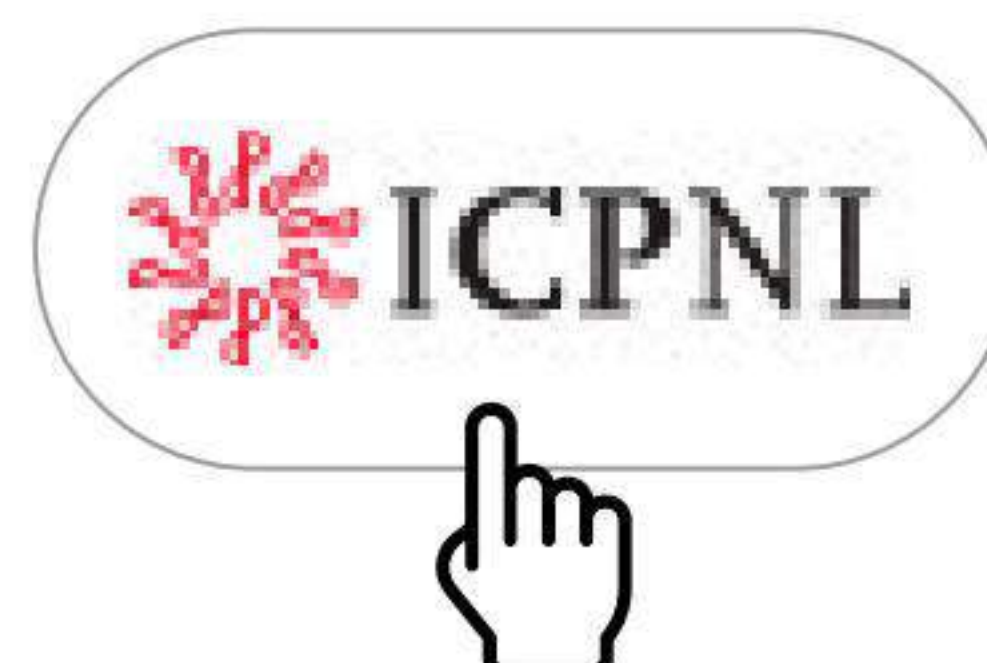
El criterio no vinculativo fiscal (44/ISR/NV), publicado en el Diario Oficial de la Federación el 11 de octubre de 2024, señala que para la deducción de erogaciones por concepto de prestación de servicios es necesaria la efectiva existencia del servicio antes de verificar el requisito de estricta indispensabilidad, de lo contrario, se consideraría una práctica fiscal indebida. Esta exigencia de materialidad se ha estado observado en el ejercicio de facultades de comprobación y en las revisiones para determinar la procedencia de la devolución de saldos a favor.

La pregunta ante esta evolución fiscalizadora es ¿Qué es y cómo se acredita la materialidad? La primera, con base en el Código Civil Federal, consiste en la existencia del consentimiento entre las partes (contrato) y la existencia del objeto materia del consentimiento (bien o servicio). Y acreditar la materialidad, es una labor de probanza, sin embargo, el SAT no se ha limitado en el estándar de probanza.

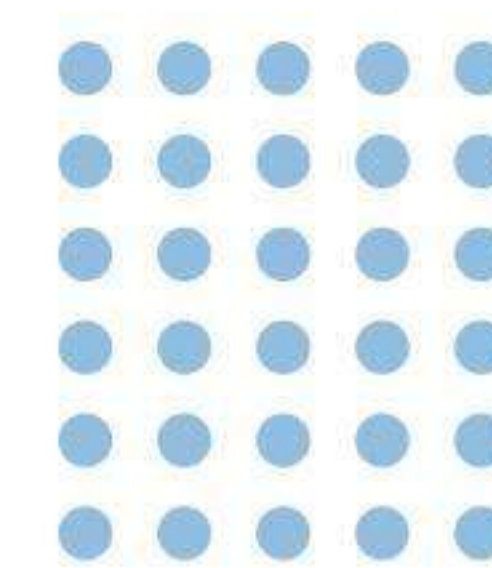
Tribunales Colegiados de Circuito han establecido criterios para la probanza de la materialidad de las operaciones para efectos fiscales, señalando que existen operaciones no complejas y operaciones complejas o especializadas; a las primeras sin que se les deba exigir mayor probanza que lo objetivo y razonable, observando el principio ontológico de la prueba: “lo ordinario se presume y lo extraordinario se acredita”.

Luego entonces, acreditar la materialidad exigida por el SAT es una oportunidad para desarrollar una metodología de probanza, apoyándose en las pruebas reconocidas por la ley, porque ya no basta solo el CFDI.

Artículo publicado originalmente en el [sitio en internet del ICPNL](#).



¿Qué es el Sistema de Información de Subcontratación (SISUB)?



Infonavit



Por la exigencia de transparencia y cumplimiento normativo que tiene el actual mundo empresarial especialmente en esquemas de subcontratación surge el **Sistema de Información de Subcontratación (SISUB)**, como una herramienta clave para las empresas aportantes registradas ante la **Secretaría del Trabajo y Previsión Social (STPS)** que operan bajo esquemas de subcontratación de personal.

Con este sistema electrónico, disponible en el **Portal Empresarial del INFONAVIT**, se facilita el cumplimiento de las obligaciones establecidas en el artículo 29-bis de la Ley del INFONAVIT y el artículo 15 de la Ley Federal del Trabajo.

El SISUB:

- Asegura que las empresas cumplan con sus responsabilidades fiscales en materia de vivienda.
- Protege los derechos de los trabajadores contratados bajo estos esquemas.

Beneficios del SISUB:

- **Gestión digital:** No es necesario acudir físicamente a oficinas.
- **Seguimiento en línea:** Se puede consultar el progreso de su solicitud en cualquier momento.
- **Notificaciones automáticas:** El sistema mantiene informada a las empresas a través del envío de correos electrónicos con su actualización.



¿Cuándo debe cumplirse?

El envío de información debe realizarse en los siguientes periodos:

Cuatrimestre	Periodo de presentación
1° cuatrimestre (enero a abril)	1 al 17 de mayo
2° cuatrimestre (mayo a agosto)	1 al 17 de septiembre
3° cuatrimestre (septiembre a diciembre)	1 al 17 de enero (del siguiente año)

¿Cómo presentar la información en el SISUB?

1. Accede al Portal Empresarial e inicia sesión con el NRP principal en:
<https://empresarios.infonavit.org.mx>
2. En la sección "Mis trámites", elige la opción "SISUB".
3. Acepta los términos y condiciones del servicio.
4. Ingresa tu e.firma.
5. Presenta el informe:
 - Si no hubo actividad, elige "Presentar Informe sin actividad", completa los datos solicitados y sube los documentos requeridos.
 - Si hubo actividad, selecciona "Presentar Informe con contratos", descarga los formatos XLS, rellena los campos necesarios y cárgalos en formato CSV.
6. Sigue las instrucciones del Instructivo de llenado archivos XLS SISUB y carga los archivos.
7. El sistema enviará una confirmación al correo electrónico registrado.

Puntos importantes a considerar:

NRP principal: Usa siempre el NRP principal o el que coincida con el domicilio fiscal.

Unificación por RFC: Agrupa la información de todos los NRP asociados al mismo RFC en un solo archivo.

Contratos y documentos únicos: La documentación inicial solo se presenta una vez, salvo modificaciones o nuevos contratos.

Errores o mensajes: Consulta la sección "Mensajes" para resolver dudas o identificar problemas en la carga.

- Asegúrate de tener al menos 25 Mbps para cargas rápidas y estables.
- No dejes celdas en blanco y utiliza archivos PDF con resolución de 200 ppp.
- Revisa toda la información antes de iniciar, ya que el sistema tiene un tiempo límite de 5 minutos.

Cumplir con tus obligaciones fiscales y laborales ahora más sencillo que nunca con el Portal Empresarial del INFONAVIT. Conoce paso a paso, las instrucciones para que completes el proceso eficientemente, garantices un trámite exitoso y evita contratiempos, en la Guía de usuario y el Instructivo de llenado, disponibles en www.infonavit.org.mx.

¡Haz uso del SISUB y asegura el cumplimiento de tus obligaciones con facilidad y confianza! En el INFONAVIT, todos los trámites son gratuitos.

Recomendaciones técnicas:





comercio
digital 

sw.
sapien
soluciones de TI

 InvoiceOne

 Tralix

 ATEB


PRODITMA

MASTEREDI 

 digifact

 Timbox
Innovación Fiscal

 quadrum

 ESTELA
WE HAVE YOU COVERED

Carvajal 
TECNOLOGÍA Y SERVICIOS

CONTPAQi
Software empresarial fácil y completo

interfactura.

 XPD
FACTURACIÓN RÁPIDA Y FÁCIL

diverza 

amexipac.org



DA ASESORAMIENTO ASESORAMIENTO ASESORAMIENTO ASESORAMIENTO

GRUPO DE PASDEL GRUPO DE PASDEL GRUPO DE PASDEL GRUPO DE PASDEL

de pasdel Grupo de pasdel Grupo de pasdel Grupo de pasdel Grupo

o, no obligatorio, no obligatorio, no obligatorio, no obligatorio,

gatorio, tiempo gatorio, tiempo gatorio, tiempo gatorio, tiempo